



RF01

0430
#3
BT
4.26.02

520.41252X00

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant(s): YQSHIMURA, et al
Serial No.: 10 / 080,715
Filed: FEBRUARY 25, 2002
Title: COMPUTER RESOURCE ALLOCATING METHOD

2152

LETTER CLAIMING RIGHT OF PRIORITY

Assistant Commissioner for
Patents
Washington, D.C. 20231

RECEIVED

MARCH 18, 2002

APR 23 2002

Technology Center 2100

Sir:

Under the provisions of 35 USC 119 and 37 CFR 1.55, the applicant(s) hereby claim(s)
the right of priority based on:

Japanese Patent Application No. 2001-312115
Filed: OCTOBER 10, 2001

A certified copy of said Japanese Patent Application is attached.

Respectfully submitted,

ANTONELLI, TERRY, STOUT & KRAUS, LLP

Carl I. Brundidge
Registration No. 29,621

CIB/rp
Attachment



日本国特許庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されて
いる事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed
with this Office

出願年月日

Date of Application:

2001年10月10日

出願番号

Application Number:

特願2001-312115

ST.10/C]:

[JP2001-312115]

願人

Applicant(s):

株式会社日立製作所

RECEIVED

APR 23 2002

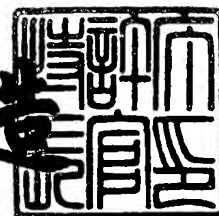
Technology Center 2100

CERTIFIED COPY OF
PRIORITY DOCUMENT

2002年 3月 1日

特許庁長官
Commissioner,
Japan Patent Office

及川耕造



出証番号 出証特2002-3011682

【書類名】 特許願

【整理番号】 H01004541A

【あて先】 特許庁長官 殿

【国際特許分類】 G06F 13/00

【発明者】

 【住所又は居所】 東京都国分寺市東恋ヶ窪一丁目 2 8 0 番地 株式会社日立製作所中央研究所内

 【氏名】 吉村 裕

【発明者】

 【住所又は居所】 東京都国分寺市東恋ヶ窪一丁目 2 8 0 番地 株式会社日立製作所中央研究所内

 【氏名】 垂井 俊明

【発明者】

 【住所又は居所】 東京都国分寺市東恋ヶ窪一丁目 2 8 0 番地 株式会社日立製作所中央研究所内

 【氏名】 マシエル フレデリコ

【発明者】

 【住所又は居所】 東京都国分寺市東恋ヶ窪一丁目 2 8 0 番地 株式会社日立製作所中央研究所内

 【氏名】 庄内 享

【特許出願人】

 【識別番号】 000005108

 【氏名又は名称】 株式会社 日立製作所

【代理人】

 【識別番号】 100075096

 【弁理士】

 【氏名又は名称】 作田 康夫

 【電話番号】 03-3212-1111

【手数料の表示】

【予納台帳番号】 013088

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【ブループの要否】 要

【書類名】 明細書

【発明の名称】 計算機資源割当方法

【特許請求の範囲】

【請求項 1】

相互にローカルネットワークで接続される複数のサーバを有し、外部にはインターネットが接続され、ストレージ及びストレージネットワークが接続された、複数ユーザの要求を処理する計算機システムにおいて、各ユーザへサーバ群を割り当てる計算機資源割当方法であって、

各ユーザごとに、そのユーザに割り当てられたサーバ群への接続、およびそれらサーバ群の間の接続に関わる VLAN を設定し、

各サーバの負荷をモニタリングし、

上記負荷のモニタリングの結果に応じて、前記ユーザの前記サーバ群の割当変更を行う際に、各ユーザに割り当てられた計算機が常に該ユーザの VLAN に入るように、割当を変更したユーザの VLAN の動的変更を行うことを特徴とする計算機資源割当方法。

【請求項 2】

上記インターネット上でキャリアを介してユーザの出口と上記計算機システムの入り口とを接続する VPN を各ユーザ毎に設定し、上記ユーザ毎に設定された VLAN では、VLAN タギングによりその VLAN を伝達するパケットを選別することを特徴とする請求項 1 の計算機資源分割当方法。

【請求項 3】

上記インターネット上でキャリアを介してユーザの出口と上記計算機システムの入り口とを接続する VPN を各ユーザ毎に設定し、少なくとも上記計算機システムの入り口にて各ユーザに設定された VPN のネットワーク負荷をモニタリングし、

上記負荷のモニタリングの結果に応じてネットワーク帯域幅を変更するよう VPN の設定変更を行うことを手順を更に有する請求項 1 の計算機資源分割当方法。

【請求項 4】

上記ストレージネットワークで各ユーザごとにゾーニングを設定し、各ユーザにストレージアクセス帯域資源を割当て、各ユーザのストレージネットワークの負荷に応じてストレージネットワークの帯域及びLUNのアクセス優先度を動的に変更する手順をさらに有する請求項3の計算機資源割当方法。

【請求項5】

ユーザに対して分割した資源に関して、ネットワーク及びサーバへの負荷が増大した場合に、ストレージネットワーク部分の資源割当の変更、VLAN部分の設定変更、VPN部分の設定変更という順番に変更することを特徴とする請求項4の計算機資源割当方法。

【請求項6】

ユーザに対して分割した資源に関して、ネットワーク及びサーバへの負荷が減少した場合に、VPN部分の設定変更、VLAN部分の設定変更、ストレージネットワーク部分の資源割当の変更という順番に変更することを特徴とする請求項4の計算機資源割当方法。

【請求項7】

ユーザに対して分割した資源に関して、サーバの負荷が増大した場合に、ユーザに対してサーバを割り当てる変更を行う時に、ユーザへのサーバの追加処理を行い、その後、VLAN部分の変更処理をストレージ側のスイッチ、サーバ群入口のスイッチの順番にステップを経て行うことを特徴とする請求項1の計算機資源割当方法。

【請求項8】

各ユーザのネットワーク負荷をユーザ出口、キャリア、サーバ群入口の少なくとも一箇所でモニタリングし、モニタリングした結果を上記計算機システム内の管理サーバで判断し、それぞれの場所のネットワーク帯域幅に対して上記計算機システム内の管理サーバにより動的な変更指示を出すことを特徴とする請求項3の計算機資源割当方法。

【請求項9】

上記キャリアと上記計算機システムが同一の管理サーバで管理される場合に、各

ユーザのネットワーク負荷をユーザ出口とキャリア入口とでモニタリングし、各測定場所におけるネットワーク帯域幅を動的に変更することを特徴とする請求項3の計算機資源割当方法。

【請求項10】

あるユーザに関して、インターネットのネットワーク負荷が増大した場合に、該ユーザに対してネットワーク帯域幅を追加割当てする変更を行う時に、VPN部分の設定変更を上記計算機システム入口、キャリア、ユーザの順番に行うことを特徴とする請求項3の計算機資源割当方法。

【請求項11】

あるユーザに関して、インターネットのネットワーク負荷が増大した場合に、該ユーザに対してネットワーク帯域幅を削減する変更を行う時に、VPN部分の設定変更をユーザ、キャリア、上記計算機システム入口の順番に行うことを特徴とする請求項3の計算機資源割当方法。

【請求項12】

上記ストレージネットワーク負荷が増大した場合に、ストレージネットワークの設定変更を、LUNのアクセス優先度の変更、ストレージネットワークの帯域変更の順番に行うことを特徴とする請求項4の計算機資源割当方法。

【請求項13】

上記ストレージネットワーク負荷が減少した場合に、ストレージネットワークの設定変更をストレージネットワークの帯域変更、LUNのアクセス優先度の変更の順番にステップを経て行うことを特徴とする請求項4の計算機資源割当方法。

【請求項14】

相互にローカルネットワークで結合される複数段の計算機を有し、外部にはインターネット接続され、ストレージ及びストレージネットワークが接続され、前記複数段の計算機の少なくとも一つは、それぞれの計算機資源の分割割当が設定され、互いに独立のOSで動作する複数の論理パーティションを形成するように構成された計算機システムにおいて、

上記インターネットでは、各ユーザに独立にVPNを設定して各ユーザにネットワーク帯域幅を割当て、

上記複数の論理パーティションを形成する計算機では、各ユーザに独立に論理パーティションを割当て、

各ユーザに割当てた論理パーティションへの接続および各ユーザに割当てた論理パーティション同士の接続に関わる各ユーザ毎のVLANを設定し、

各VLANではVLANタギングによりそのVLANを伝達するパケットを選別することを特徴とする計算機資源割当方法。

【請求項 1 5】

上記ストレージネットワークでは、計算機の論理パーティションに対応して各ユーザごとにゾーニングを設定し、もって計算機からストレージ資源までユーザのセキュリティを確保することを特徴とする請求項 1 4 の計算機資源割当方法。

【請求項 1 6】

相互にローカルネットワークで接続される複数のサーバを有し、外部にはインターネット接続され、ストレージ及びストレージネットワークが接続された、複数ユーザの要求を処理するシステムにおいて、各ユーザへ課金を行う課金方法であって、

各ユーザごとに、そのユーザに割り当てられたサーバ群への接続、およびそれらサーバ群の間の接続に関わるVLANを設定し、

予めユーザ毎に設定されたサービスレベルとそのユーザに割り当てられたサーバ群の稼働状況との比較に応じて各ユーザのサーバ群の割当を随時変更し、サーバ群の割当実績に従って課金する課金方法。

【請求項 1 7】

ユーザごとに設定されたサービスレベルとストレージネットワークの稼働状況との比較に応じて各ユーザのストレージネットワーク帯域幅の割当もしくはストレージのアクセス優先度を随時変更する手順を更に有し、ストレージネットワークの稼働実績に基づき課金金額を算出することを特徴とする請求項 1 6 の課金方法。

【請求項 1 8】

予めユーザごとに設定されたサービスレベルとネットワークの稼働状況との比較に応じて各ユーザのネットワーク帯域幅の割当を随時変更する手順を更に有し、

ネットワークの稼働実績に基づき課金金額を算出することを特徴とする請求項 16 の課金方法。

【請求項 19】

各ユーザのサーバの稼働実績に基づく課金金額を基本とし、オプションとして V P N、V L A N 及びゾーニングによってユーザ毎のセキュリティ確保を行う契約条件がある場合にサーバの使用料金に追加料金を課すことを特徴とする請求項 16 の課金方法。

【請求項 20】

オプションとして各ユーザが使用するネットワーク帯域幅の保証を行う契約条件がある場合にネットワーク帯域幅の使用料金に追加料金を更に課すことを特徴とする請求項 18 の課金方法。

【請求項 21】

相互にローカルネットワークで結合される複数段の計算機を有し、外部にはインターネット接続され、ストレージ及びストレージネットワークが接続され、前記複数段の計算機の少なくとも一つは、それぞれの計算機資源の分割割当が設定され、互いに独立の O S で動作する複数の論理パーティションを形成するように構成された計算機システムにける各ユーザへの課金方法であって

予めユーザごとに設定されたサービスレベルと計算機資源の稼働状況との比較に応じて各ユーザの計算機資源割当を随時変更し、

各ユーザの計算機資源の稼働実績に基づく課金金額を基本とし、

オプションとして V P N、V L A N 及びゾーニングによってユーザ毎のセキュリティ確保を行う契約条件の有無によって追加料金を課す課金方法。

【請求項 22】

相互にローカルネットワークで結合される複数段の計算機を有し、外部にはインターネット接続され、ストレージ及びストレージネットワークが接続され、前記複数段の計算機の少なくとも一つは、それぞれの計算機資源の分割割当が設定され、互いに独立の O S で動作する複数の論理パーティションを形成するように構成された計算機システムにおける各ユーザへの課金方法であって、

上記インターネットでは、各ユーザに独立に V P N を設定して各ユーザにネット

ワーク帯域幅を割当て、

予めユーザごとに設定されたサービスレベルとネットワーク帯域の稼働状況との比較に応じて各ユーザのネットワーク帯域幅の割り当てを随時変更し、稼働実績に基づき課金金額を算出することを特徴とする課金方法。

【請求項 2 3】

オプションとして各ユーザが使用するネットワーク帯域幅の保証を行う契約条件の有無によってネットワーク帯域幅の使用について追加料金を更に課すことを特徴とする請求項 2 2 の課金方法。

【請求項 2 4】

相互にローカルネットワークで接続される複数のサーバを有し、外部にはインターネット接続され、ストレージ及びストレージネットワークが接続された、複数ユーザの要求を処理するシステムにおいて、各ユーザへサーバ群を割り当てる計算機資源割当方法であって、

上記インターネットではユーザ出口と、キャリアと、上記サーバ群の間でユーザ毎にVPNが設定され、かつ各ユーザのネットワーク帯域が割り当てられ、ユーザ出口、キャリア、サーバ群入口において各ユーザに割当てたネットワーク帯域幅を負荷に応じて動的に変更し、

かつ契約時に帯域保証サービスを希望したユーザに対してはそれ以外のユーザと比較して優先して割当変更を行う計算機資源割当方法。

【発明の詳細な説明】

【0 0 0 1】

【発明の属する技術分野】

本発明は、計算機システム内の資源をユーザごとに分割して割当る方法に係り、特に相互にネットワークで結合される複数の計算機からなるシステムにおいて、複数ユーザの要求を処理する際に、各ユーザとの間であらかじめ取り決めたサービス内容に関する契約を維持するために必要な計算資源をリアルタイムに提供し、かつユーザ間のセキュリティを保持するための資源割当方法に関する。

【0 0 0 2】

【従来の技術】

情報部門のコスト削減のために、企業内情報システム運用や企業のホームページ管理をASP（アプリケーション・サービス・プロバイダ）業者にアウトソースする事業形態が増加している。ASP業者はさらにデータセンタ業者に計算機資源供の供給、運用管理をアウトソースする形態が多い。

【0003】

データセンタ業者は、多数の計算機資源を用意して複数のユーザ企業に分割使用させることにより、自身の運用コストを削減し、低価格のサービスをユーザ企業に提供する。ユーザ企業間のセキュリティを保持するため、一般には各ユーザ企業ごとに異なる計算機資源およびストレージ資源を割り当てることが多い。

【0004】

またユーザ企業の負荷は時間帯、季節等により変動するため、負荷に応じて割当て資源を増減させる契約形態も多い。特に企業のホームページ管理を請け負っている場合などは、不特定多数の消費者がインターネット経由でアクセスするため負荷の予測がつきにくい。これに対してはユーザ企業側でたとえば新製品発表による負荷増を予測してあらかじめ決めた台数の計算機資源をある一定期間増強するようデータセンタ業者と契約する。データセンタ業者は、増強した計算機資源を、別の期間は別のユーザ企業に割り当てることにより資源の有効活用を図る。このような構成変更を容易にするために、負荷分散装置を複数の計算機資源の前段に配置し、ある期間はユーザ企業Aに、別の期間はユーザ企業Bに計算機資源を使用させるように、データセンタを構成する。負荷分散装置の例としては、アルテオン社のACE directorなどが挙げられる（日経オープンシステムズ 1999. 12 no. 81 pp. 128-131）。負荷分散装置の設定は上記の契約に基づきあらかじめ人手で設定する。またストレージ資源を増強する必要がある場合は、ストレージの内容を複製を行う必要がある。

【0005】

さらに、データセンタでは多数のユーザ企業に異なる計算機資源を提供するため、多数の計算機資源を管理する必要が生じ管理コストが増大する。そこで1台あたりの性能が高い計算機資源、たとえば高多重SMP計算機を数少なく導入し、それを複数ユーザ企業が共有するように制御する方法が考えられる。ユーザ企

業間のセキュリティを保持するため仮想計算機の機能を利用する。仮想計算機の例としては、日立のプロセッサ資源分割管理機構PRMFがあげられる（HITACマニュアル 8080-2-148-60）。PRMFでは、1つの計算機上で複数のOS（オペレーティング・システム）が動作し、OSごとに独立の資源、たとえば主記憶、ネットワークアダプタなどが割り当てられる。OS間で資源を共有しないため、異なるOS上で実行される異なるユーザ企業のプログラム間のセキュリティは保持される。またPRMFでは、OSごとに割り当てるCPU資源の比率を制御できるように構成されているが、あらかじめ計画した比率変更のみ可能である。

【0006】

一般にデータセンタは複数ユーザが利用しており、ユーザ毎のデータの独立性を保つようなセキュリティ確保の技術が考えられている。現在主に知られているセキュリティの技術としては、VLAN(アスキー社VPN/VLAN教科書pp31-pp42)やVPN(アスキー社VPN/VLAN教科書pp7-pp30)、FCゾーニング(ピアソン・エデュケーション社 SAN pp85-pp86)が知られている。VLAN、FCゾーニングの技術はネットワークを論理的にグループ化することを実現し、互いに他のグループにアクセスできないようにする技術である。また、VPNは暗号化とパケットの優先度制御によってユーザに対しセキュリティを確保する技術である。また、VPNにはネットワーク使用帯域を保障することも可能にする。さらに、ゾーニングの技術はユーザに割り当てられたストレージネットワークスイッチのポートについてストレージへのアクセスを制御することが可能である。例えば、ユーザAはストレージに対するユーザ全体のアクセス回数で10回のうち3回の割合でLUNにアクセスするのを、10回のうち5回の割合でLUNにアクセスするというようにアクセス優先度を増やすことで、負荷増大に対処できる。このセキュリティ技術によって、ユーザはデータセンタ内の計算機資源中のユーザ専用データにセキュリティの不安なくアクセスして利用できる。VLANやVPN、FCゾーニングはネットワーク管理者が通常予め計画して静的に設定し必要時以外は設定変更しない。

【0007】

最後にASP、ISP（インターネット・サービス・プロバイダ）業者とユーザの間ではサービスレベル契約を結ぶことが一般的になりつつある。接続性、可用性、レイテンシ性能などのサービスレベル保証を契約する。さらに保証レベル未達の場合の補償契約を結ぶ形態も多い。

【0008】

【発明が解決しようとする課題】

上記の従来技術では、以下の問題点がある。

【0009】

負荷分散装置やネットワークスイッチの設定を契約に基づきあらかじめ人手で設定する方式では、ユーザ企業側で予測できない急速な負荷変動にリアルタイムに対応することは困難である。これはユーザ間で異なる計算機を割り当てる場合も仮想計算機を使用する場合も同様である。さらに、システムの拡張を行うと同時にユーザのネットワークセキュリティを守ることはユーザ、データセンタ双方のネットワーク管理者にとって非常に労力を割くところである。特に負荷変動によってネットワーク構成が動的に変わる環境においては、人手によってユーザのセキュリティの管理を恒常的に行うことは困難である。

【0010】

本発明の目的はネットワークが動的に変更した場合であってもユーザのセキュリティを確保し、データセンタ及びユーザの管理者の負荷を軽減するような手法を提供することである。また、ネットワークが動的に変更する時にユーザのセキュリティを守りながら、ユーザの負荷ピークに対応できるようにネットワーク構成を変更する手法を提供することおよびユーザとの間に結んだ契約内容分だけの通信帯域を確保してユーザへのWebサービスの品質を保つことである。

【0011】

【課題を解決するための手段】

本発明では、ユーザ識別表とVPN、VLANそしてストレージネットワークそれぞれの構成定義表を用意し、管理サーバにて管理する。データセンタへのユーザ要求パケットからユーザ識別表によりユーザ企業を特定する。一方、VLANの構成定義表にはユーザ毎に処理を実行すべき計算機の組を定義し、これを負

荷分散装置及びネットワークスイッチに設定する。負荷分散装置は設定された計算機の組からいずれかを選択してユーザ要求を実行させる。複数の負荷分散装置がある場合は、管理サーバは負荷分散装置間で本表が整合するよう制御する。さらに、管理サーバではネットワークの帯域や構成、各計算機の稼動状況をモニタし、サービスレベル契約を満たしているか調べ、必要であればネットワーク帯域幅や計算機資源の削減・増強を行ってユーザとの契約内容に合うようにすると共にユーザのVLANの構成を変え、セキュリティを保つ。具体的には上記の計算機の組のネットワークの構成定義表を変更して、負荷分散装置及びネットワークスイッチに再設定する。さらに管理サーバはユーザに割当てた計算機資源量やサービスレベル契約を守れたかの履歴を作成し、課金情報を作成する。

【 0 0 1 2 】

また本発明の別の実施形態では、仮想計算機機構を有する計算機でデータセンタを構成する。ユーザ企業ごとに1つのOSで制御される仮想計算機機構を与え、管理サーバはユーザ企業毎のネットワーク帯域と各計算機に各計算機機構のCPU時分割使用割当て%を動的に設定する。さらに、管理サーバではネットワーク帯域や各計算機の稼動状況をモニタし、サービスレベル契約を満たしているか調べ、必要であればネットワーク帯域幅やCPU時分割割当て%の削減・増強を行う。

【 0 0 1 3 】

【発明の実施の形態】

以下、図面を参照しながら、本発明の実施の形態を説明する。

〔 1 〕 第 1 の 実施 形 態

まず、実施形態を説明する上で必要になる主な図の説明を行う。

図1は、本発明で対象とするデータセンタが、インターネット回線会社(キャリア)(I I 0)を介してユーザ企業A(A A 0)、ユーザ企業B(B B 0)と接続されている例を示す。図2は、図1のデータセンタD D 0の内部構成を示している。ユーザA、B毎に専用のVLAN V 0 1、V 0 2が組まれている。図3、図4は本実施例におけるユーザからデータセンタまでいたるVPNの構成を示している。図5はストレージネットワークの主な構成を示している。ユーザA、B

ごとに専用のゾーンZ01、Z02が組まれている。図6はデータセンタDD0の管理サーバC0の持つサーバ割当及びVLAN関連の情報を集めた図である。また、図7はデータセンタDD0の管理サーバC0が持つVPN関連の情報を集めた図、図8、図9は夫々ユーザ帯域管理サーバC10、キャリア帯域管理サーバC20がそれぞれ持つVPN関連の情報を集めた図である。以下の説明において、ネットワークはインターネットを指すものとする。なお、キャリア等のVPNルータは図1では1つしかないように見えるが、実際には、複数台存在しても良い。その場合も制御手順は同一である。

さらに図10はデータセンタDD0の管理サーバC0が持つストレージネットワーク関連の情報を集めた図である。

図11は、第1の実現形態を説明するに際して、ユーザAが通信に用いるパケットの一覧である。図12、図13は、ユーザ企業Aが本データセンタと使用条件契約を結ぶときの入力画面の一例を示している。本例では、ユーザ企業Aはデータセンタ内のwebサーバ群、APサーバ群、DBサーバ群のすべてを使用し、ユーザ企業Aはネットワーク帯域幅として1.5Mbpsから5Mbpsを使用する契約を結んでいる。

【0014】

図14は契約を結んだユーザに対してサーバやネットワーク帯域幅をシステム立上げ時に割り当てる手順を示したものである。図15はユーザに割り当てられるネットワーク帯域幅が動的に増大・減少する時の手順を示したものであり、図16はユーザに割り当てられるサーバ台数が動的に増大・減少する時の手順を示したものである。さらに、図26は負荷が増大した場合のVLAN、VPN、ストレージネットワークの各部分に関する制御手順を示したものであり、図27は負荷が減少した場合のVLAN、VPN、ストレージネットワークの各部分に関する制御手順を示したものである。図28はユーザに割り当てられるストレージネットワークの帯域幅が動的に増大・減少する時の手順を示したものである。

さて、実施形態の説明を行う。図1のクライアントa0はA社システムのプライベート・ネットワーク・アドレスを有しており、VPN（バーチャルプライベートネットワーク）ルータA0を介してキャリアのVPNルータI01経由でデー

タセンタ内のVPNルータD0と接続する。図2は、データセンタDD0の構成を示す。本例ではユーザ要求に対しwebブラウザインターフェースを提供するwebサーバ群、webサーバを経由して発生するアプリケーションプログラムを動作させるAPサーバ群、アプリケーションプログラムからデータベースアクセス要求が出たときにそれを処理するDBサーバ群の3層構成になっている場合を示す。

【0015】

図12、13は、ユーザ企業Aが本データセンタとサービスレベル契約を結ぶときの入力画面の一例を示している。また、本例では、ユーザ企業Aのために、webサーバ、APサーバ、DBサーバいずれも必ず最低1台を割当て、またそのすべてをCPU稼働率50%未満で稼働させる。稼働率が50%以上となる場合は各webサーバ、APサーバ、DBサーバの割当て数を最大6台までは増加する契約を結んでいる。また、ネットワーク帯域における契約については図12でユーザの使用帯域幅の保証を行うか否かの選択を行い、具体的な使用帯域幅の契約は図13で行う。本例では入力画面中の使用帯域幅保証選択の欄にチェック印が入力され、具体的な帯域は最低1.5Mbpsが割当られ、帯域幅の使用率が40%未満となるように稼働させる。帯域幅の使用率が40%以上となる場合は帯域幅を最大5Mbpsまでは増加させる契約を行っている。

【0016】

上記のような入力画面による契約に基づき、A社にはwebサーバa10、APサーバa20、DBサーバa30、が与えられ、B社にはwebサーバb10、APサーバb20、DBサーバb30が与えられるものとする。本実施例においては、ユーザの各層に1台ずつのサーバしか割当てていないが、2台以上割当てられることが考えられる。またストレージs01はLUN(論理単位番号)単位でLU01がA社用に、LU02がB社にが割り当てられる。サーバ群y10、y20、y30は、A社、B社の負荷が大きくなったときに割り当てるための予備サーバ群である。なお、y10、y20、y30は1台分の表記しかしていないが、2台以上存在することが考えられる。

【0017】

A社が使用する代表IPアドレスは、webサーバがa100とする。またB社にもwebサーバb100なるIPアドレスを使用するものとする。なお、本実施例は、Webサーバ、APサーバ、DBサーバ及びクライアントは各1台として説明しているが、複数台ある場合も実施例は同様である。

【0018】

以下図を参照しながら、このデータセンタ中のサーバ群や負荷分散装置を中心とするスイッチが、ユーザAの要求をサーバ群a10、a20、a30を使用して如何に処理するかを示す。

【0019】

図1においてクライアントa0がVPNルータA0に送出した要求パケットの構成は、図11(1)1100に示すとおりである。パケットの先頭があて先サーバのアドレス、次項が送り元クライアントのアドレスである。VPNルータA0はパケットをインターネット回線I10に送出するときにVPNのカプセル化を行い、図11(2)のパケット1101を生成する。VPNルータD0ではこのパケットをアンカプセル化する。パケットのカプセル・アンカプセルの技術は公知である。

【0020】

信号線I0から入力された図11(2)のパケット1101に対しアンカプセル化を行うと図11(3)のパケット1102を生成するとともに、信号線I1を通じて負荷分散装置LB01に出力する。ユーザは負荷分散装置に設定している代表アドレスa100、b100をアクセスすることで、データセンタの管理サーバC0の持つ図6の負荷分散装置のアドレス表T00に相当する情報を負荷分散装置LB01で参照する。負荷分散装置LB01では図11(3)のパケット1102の宛先アドレスa100に対して、負荷分散装置LB01に設定されている図6のアドレス参照表T00に相当する情報と対応させて各ユーザの代表アドレス(仮想アドレス)を実サーバのアドレスa10に変換した図11(4)のパケット1103を生成する。あて先の選択および変更技術自身は公知である。また、パケット1103を対応する表T02のport#(LB01)のカラムに相当する情報を参照し、ユーザ専用のVLANに所属するポートのみに送信する。図2

では、負荷分散装置 L B 0 1 の入口 p 0 0 0 がねね、ねね、の技術で複数のユーザ（複数の V L A N）と共用している場合を示す。各ユーザにおいてデータセンタ中はユーザ専用の V L A N が組まれている。一方、V L A N タギングの技術でユーザからは V L A N 情報（V L A N タグ）を持ったパケットが流れる。V L A N 情報を持ったパケットは同じ V L A N のネットワークにのみ流れることが可能である。そのため、各ユーザのセキュリティが守られることになる。図 6 の表 T 0 2 に各ユーザとユーザに対して組まれている V L A N と V L A N 所属のサーバ及びスイッチのポートの一覧を示す。すなわち、ユーザに割当てられたサーバがどのサーバと通信できるかを示す。ここで、ユーザが複数のネットワークスイッチでそれぞれローカルに V L A N を組むが、その V L A N 設定を組み合わせることにより、複数の装置にまたがるユーザ専用の V L A N を設定することを可能にする。例えば、ユーザ A であれば、W e b サーバ a 1 0 を挟んで L B 0 1 ではポート p 0 0 1 にローカルに V L A N を組み、S W 0 1 では p 1 0 1、p 2 0 1 で同じローカルに V L A N を組み、この 2 つのローカル V L A N を同じ 1 つのグループに設定することで、L B 0 1 と S W 0 1 にまたがるユーザ専用の V L A N を実現している。この効果を例示すると、ユーザ A が W e b サーバ b 1 0 にアクセスしようとした時に、W e b サーバ b 1 0 は V L A N V 0 2 所属で、ユーザ A は V L A N V 0 1 所属であるのでアクセスは拒否される。

【 0 0 2 1 】

w e b サーバ a 1 0 はパケット図 1 1 (4) 1 1 0 3 を受け取り、W e b 処理の結果 A P サーバへのアクセスが必要になると a 2 0 へのアクセス要求であるパケット 1 1 0 4 （図 1 1 (4) ）を生成する。本パケットはポート p 1 0 1 を介してネットワークスイッチ S W 0 1 に受け取られる。ネットワークスイッチ S W 0 1 は図 6 の V L A N 構成表 T 0 2 の port # (S W 0 1) のカラムに相当する情報、すなわち、p 1 0 1、p 2 0 1 が同一の V L A N に所属するように設定されるので、宛先アドレス a 2 0 にパケット 1 1 0 4 （図 1 1 (4) ）を送り届けることができる。

【 0 0 2 2 】

以下同様に A P サーバ a 2 0 がパケット 1 1 0 5 を生成して、D B サーバ a 3

0で処理が行われる。DBサーバa 3 0からAPサーバa 2 0、Webサーバa 1 0、クライアントa 0に返答が返るのも同様であり、順次パケット1 1 0 6～1 1 1 0が生成される。VLANの構成についても同様である。

【0 0 2 3】

ユーザ企業Bからの要求があった場合は、上記と同じ手順でVPNルータD 0及び負荷分散装置L B 0 1を通過して、同様にサーバ群b 1 0、b 2 0、b 3 0で処理されることとなる。(パケット形式は同様なので図示しない。)

以上により、ユーザAとBの処理を実行するサーバ群はサーバa 1 0、a 2 0、a 3 0が属するVLANとb 1 0、b 2 0、b 3 0が属するVLANに各々分割される。

【0 0 2 4】

なお、本説明ではユーザA、B共に図1 2でセキュリティサービスを希望してユーザ専用のVLANを組んだ場合を考えている。図1 2でセキュリティサービスを希望した場合は、各々のユーザに対して専用のVLANが生まれ、希望していない場合はユーザ共用のVLANでサービスを受けることとなる。

【0 0 2 5】

図2において、管理サーバC 0は信号線L 0 1～L 0 8を介してサーバ群、負荷分散装置、VPNルータ、ネットワークスイッチの動作状況をモニタリングしている。モニタリングの内容はユーザとのサービスレベル契約の内容による。たとえばCPU稼働率などである。またモニタリングプログラムは管理サーバC 0で動作してもよいし、各サーバ群、負荷分散装置上で動作してもよい。また管理サーバC 0は信号線L 0 1を介してVPNルータD 0からユーザごとのネットワーク帯域使用に関する稼働表(VPN稼働状況表)図7のT 0 5の内容を入手する。

【0 0 2 6】

図6はサーバ構成及びVLAN構成について管理サーバC 0が持つ情報を示した図である。ネットワーク帯域等のVPN関連の情報やストレージネットワーク関連の情報に関しては後述する。図6のT 0 1はユーザ条件設定表であり、制御プログラムP 1 0が図1 2、図1 3のサービスレベル条件入力画面に基づき設定する。その後、図6のT 0 1の情報に基づきT 0 2のサーバ及びVLAN構成表

が作成される。この場合、A社のユーザに対してはWebサーバ、APサーバ、DBサーバいずれも最低1台を与え、与えたすべてのサーバでCPU稼働率50%未満でプログラムを動作させ、それに違反しそうな場合は6台まではサーバ数を増加する契約となっている。またB社のユーザに対しても同様に、Webサーバ、APサーバ、DBサーバいずれも最低1台を与え、CPU稼働率50%未満でプログラムを動作させ、それに違反しそうな場合は6台まではサーバ数を増加する契約となっている。また、T02では図12で入力したセキュリティオプションの項目の情報を保持しており、項目にチェックした場合はユーザの専用のVLANを組むことにする。

制御プログラムP10はモニタリング結果と図6のユーザ条件設定表T01を照合し、現在の資源割当てがサービスレベル契約を満たしているかを調べ、その結果を図6のサーバ及びVLAN稼働表T03に格納する。図6のサーバ及びVLAN格納表T03には、ユーザAに対して現在割当てられているサーバの一覧、各割当台数における割当時間の履歴のカラム、ユーザAに与えた全てのサーバに関してサービスレベルで設定したCPU稼働率以上で稼働していた時間の合計及びそれ未満で稼働していた時間の合計履歴のカラムが記録される。ここで、CPU稼働率以上のカラムはユーザが契約した最大のサーバ台数で処理できない負荷が入った場合やサーバを割当てようとしたが予備サーバが不足していて割り当てられなかった場合に記録される。モニタリング結果がサービスレベル契約を満たしていない場合は、制御プログラムP10は割当てサーバを増やす。サーバ割当てを管理するために、どのユーザにどのサーバを与えたかを示す図6のVLAN構成表T02のサーバのカラムや、ユーザが認識している仮想サーバ名と与えた実サーバの対応表である負荷分散装置のアドレス対応表T00を保持している。また図6のサーバ及びVLAN稼働表T03にはサーバ割当台数履歴、リソース不足時間等の課金に関する情報もあわせて記録している。課金に関しては後述する。

【0027】

上記制御を行うために、制御プログラムP10がシステム立上げ時に資源を分割する手順を図14を用いて説明する。

【 0 0 2 8 】

最初に図 1 2、図 1 3 のサービスレベル条件入力画面に示される情報を入力し（1 4 0 1）、データセンタの管理サーバ C 0 は、ユーザ条件設定表 T 0 1 を作成する（1 4 0 2）。

【 0 0 2 9 】

さらに図 1 3 のサービスレベル条件入力画面に示される情報を入力し、ユーザが入力した仮想アドレスによってサーバアドレス対応表 T 0 0 中の仮想 a d d r 欄を作成する（1 4 0 3）。続いてサーバの割当てを、w e b サーバ群、A P サーバ群、D B サーバ群ごとに行い、ユーザ専用の V L A N の設定を行う。同時に、ユーザに割当てするネットワーク帯域やストレージ(L U N)の設定を行う。具体的には、ユーザ条件設定表 T 0 1 を参照して各ユーザに最低 1 台ずつサーバを与えるべきことを検出すると、サーバを確保して、確保したサーバを V L A N 構成表 T 0 2 の割当サーバのカラムに記述する（1 4 0 4）、また、サーバに繋がる後段のポート、前段のポートを V L A N 構成表 T 0 2 の port# のカラムに記述し、各ネットワークスイッチ S W 0 1 ～ 0 2 に V L A N 設定指示を出す。例えば、ユーザ A の場合であればネットワークスイッチ S W 0 1 に対して、ポート p 1 0 1 とポート p 2 0 1 が同じ V L A N に所属するように V L A N 設定指示を出すというような形の指示である。その後、サーバアドレス対応表 T 0 0 の実 a d d r 欄を作成する（1 4 0 5）。続いてユーザ条件設定表 T 0 1 に基づき、V P N 設定表 T 0 4、ストレージネットワーク構成表 T 0 6 を作成した後、ネットワーク及びストレージネットワークの帯域幅を確保し、V P N 設定表 T 0 4 の帯域幅のカラム及びストレージネットワーク設定表 T 0 6 の帯域幅のカラムに記述し、データセンタ管理サーバはユーザ管理サーバ及びキャリア管理サーバに対して帯域幅設定指示を出し、各 V P N ルータに帯域幅を設定する（1 4 0 6）。具体的には T 0 1 中の V P N の最小・最大帯域幅、帯域利用率の閾値、保証帯域幅のカラム中の情報を信号線 L 0 を介してユーザ帯域管理サーバに送る。ユーザ帯域管理サーバにおいてはユーザ条件設定表 T 0 1 の最小・最大帯域幅、帯域使用率、保証帯域幅のカラム中の情報を用いて V P N 設定表 T 0 8 を作成し、V P N ルータ A 0、B 0 に設定する。キャリアの帯域管理サーバでも同様に V P N 設定表 T 1

0を作成し、VPNルータI01に設定する。

最後に作成したサーバアドレス対応表T00のコピーを信号線L02を介して負荷分散装置LB01に設定する(1407)。

【0030】

さらに、ユーザ条件設定表T01に基づき、図6のサーバ及びVLAN稼働表T03、図7のVPN稼働表T05、図8のストレージネットワーク稼働表T07を作成する(1408)。具体的には、ユーザAに対するCPU稼働率履歴やネットワーク帯域使用率履歴を記録する欄を作成する。

【0031】

以上により資源分割制御に必要な情報が生成され、VPNルータD0、ネットワークスイッチSW01～03に設定され、正しく資源分割された状態でシステムが動作開始できる。

【0032】

続いて以下に、制御プログラムP10が負荷変動時にサーバ割当てを変更する手順を図16を用いて説明する。Webサーバを例に挙げて説明する。

【0033】

前述したように信号線L01～L08を介して全ユーザに対して各サーバの稼働情報をモニタし(1601)、各ユーザごとに稼働情報を集計して図6のサーバ及びVLAN稼働表T03に格納し(1602)、図6のユーザ条件設定表T01と比較した後(1603)、まずサービスレベル契約に照らしてサーバを削減できないか検討する(1604)。削減可能かどうかの判断方法の1例としては、CPU稼働率とサーバ台数の積に対して比例計算を行う方法が挙げられる。たとえばユーザAのサービスレベル条件はCPU稼働率50%未満であるが、現在4台がwebサーバとして与えられており、いずれもCPU稼働率が25%未満であれば、webサーバ数を2台まで削減してよいと判断できる。複数のユーザが存在する場合はまず、全ユーザについてサーバ削減処理を行った後に、全ユーザのサーバ増強処理を行う。ここでは、Webサーバa10を削減することとする。削減可能であれば、まず、アドレス対応表T00の実addrのカラムからサーバa10を削除し、実addrのカラムの内容を設定するように負荷分散装置LB

01に対して指示する。管理サーバのVLAN構成表T02において、port#(LB01)、port#(SW01)のカラムから削除するサーバa10につながるポートp001、p101を削除する。

その後、Webサーバa10に接続されているLB01のポートp001をVLANから削除したあとにSW01のポートp101をVLANから削除する処理を行うというように、前段のスイッチのVLAN変更処理が終わった後に後段のスイッチのVLAN変更処理を行う(1605)。

次に、削減処理を通知されたサーバa10はプログラムの処理を終了して、使用している資源を解放する。すなわちコンテンツの切り替えやディスクキャッシュの消去などを行う(1606)。

解放が終了すると削減されたサーバは管理サーバC0にその旨通知するので、管理サーバC0はそれを待って、図6のVLAN構成表T02のWebサーバのカラムを変更する。また、サーバ及びVLAN稼働表T03においてサーバ台数の履歴などの課金情報のパラメータを変更する(1607)。なお、本例では、T03のサーバ割当履歴表のサーバ台数履歴のカラムにおいてはwebサーバ群、APサーバ群、DBサーバ群の割当て履歴を区別して記録しているので、群ごとに単価を変えておき群ごとの割当て数と割当て時間履歴と各単価の積で課金を計算することも可能である。以上、例としてWebサーバを挙げたが、他のサーバの場合は負荷分散装置に対する実アドレス変更指示が無く、代わりにアプリケーションに何らかの方法でサーバを削減することを通知し、ネットワークスイッチのポートに対するVLAN変更のみを行う。

【0034】

図16の説明に戻る。つづいてサーバ数を増強する必要があるかを検討する(1608)。何台増強すべきかの判断は、削減時と同様に比例計算である。増強する必要があるれば、webサーバ、APサーバ、DBサーバ群ごとに割り当てられる空きサーバがあるかをVLAN構成表T02を参照して調査する(1609)。もし空きサーバがなければ運用管理者に通知し、リソースが足りなくてサーバが割当られないためのサービスレベル未達かユーザの契約条件を超えてしまったためのサービスレベル未達か区別して記録される(1610)。空きサーバが

あればユーザに割当て対象の空きサーバ y 1 0 から必要な台数を選択し、ユーザに割当てする (1 6 1 1)。その後、図 6 の V L A N 構成表 T 0 2 の W e b サーバのカラムに割当てられたサーバを追加する。次に管理サーバの V L A N 構成表 T 0 2 に対して port# (S W 0 1)、port# (L B 0 1) のカラムを変更し、負荷分散装置 L B 0 1 に port# (L B 0 1) のカラムの内容を、ネットワークスイッチ S W 0 1 に対して port# (S W 0 1) のカラムの内容を設定するよう変更する。

その後、割当て対象のサーバ y 1 0 に接続されているスイッチのポートを S W 0 1 側では p 1 0 3、L B 0 1 側では p 0 0 3 の順に V L A N に割当てるというように W e b サーバが接続されている後段のポート、前段のポートの順番でユーザの V L A N を変更する (1 6 1 2)。最後にデータセンタの管理サーバ C 0 は負荷分散装置のアドレス対応表 T 0 0 について実 Addr のカラムに y 1 0 を追加する変更を行い、負荷分散装置 L B 0 1 に設定するよう指示する。負荷分散装置 L B 0 1、ネットワークスイッチ S W 0 1 の内容が変更されたことを確認してから、割当サーバ台数などの課金情報に関するパラメータを変更する (1 6 1 3)。

今回は、例として W e b サーバを扱ったので、変更の過程で負荷分散装置のアドレス対応表の変更について考える必要がある。A P 及び D B サーバの場合は負荷分散装置の設定変更はせず、代わりにアプリケーションに何らかの方法でサーバを削減することを通知し、ネットワークスイッチのポートに関する V L A N の変更のみで良い。

【 0 0 3 5 】

以上は管理サーバ C 0 上の制御プログラム P 1 0 の手順である。

本変更方式の利点としては、全ユーザに対してサーバの割当増加指示を行う前にユーザからのサーバの割当削減指示を行うので、データセンタ内のサーバ資源の使用率が良い点である。この順番を守らず、ユーザに対するサーバの追加を先に行った場合は一時的に予備サーバが不足する事態が考えられる。その後のサーバ削減処理においてユーザのサーバ使用率が低いサーバが削減される可能性があり、サーバ資源を効率的に使っているとは言い難い。以下、ネットワークの帯域幅の割当やストレージネットワークの帯域幅の割当についても同様に考えられる。

【 0 0 3 6 】

さて、制御プログラム P 1 0 が負荷変動時にインターネットのネットワーク帯域の割当を変更する手順を図 1 5 を用いて説明する。これは、ユーザとデータセンタ間の間での V P N の実現方法によって 3 つの場合がある。V P N における帯域幅の変更方法については、公知である。ここで、データセンタ管理サーバが持つ情報について説明する。

図 7 において、ユーザ条件設定表 T 0 1 のうち V P N に関する情報は、最小帯域幅・最大帯域幅、帯域利用率の閾値のカラムである。V L A N 設定表 T 0 4 は、ユーザ条件設定表 T 0 1 を参照して作成される最小帯域幅、最大帯域幅、帯域利用率についてユーザが設定した条件を保持する表であり、これを用いてネットワークの帯域についてのサービスレベル条件が満たされているかを判断する。さらに V P N 稼動状況表 T 0 5 にはユーザ、キャリア、データセンタの各 V P N ルータにおいてユーザに割り当てられた帯域幅について、帯域使用率を満たしている時間そして満たせなかった時間の履歴、そして、最小帯域幅から最大帯域幅までユーザに割当られた帯域幅の履歴のカラムが存在している。

図 8 はユーザの帯域管理サーバが V P N ルータについて保持している情報についてまとめた図で、V P N 設定表 T 0 8 は最小帯域幅、最大帯域幅、帯域利用率についてユーザに設定された条件を保持する表である。さらに V P N 稼動状況表 T 0 9 にはユーザの V P N ルータにおいてユーザに割り当てられた帯域幅について、帯域使用率を満たしている時間そして満たせなかった時間の履歴、そして、最小帯域幅から最大帯域幅までユーザに割当られた正規化された帯域幅の履歴のカラムが存在している。さらに、図 9 はキャリアの帯域管理サーバが V P N ルータについて保持している情報についてまとめた図で、V P N 設定表 T 1 0 は最小帯域幅、最大帯域幅、帯域利用率についてユーザに設定された条件を保持する表である。さらに V P N 稼動状況表 T 1 1 にはキャリアの V P N ルータにおいてユーザに割り当てられた帯域幅について、帯域使用率を満たしている時間そして満たせなかった時間の履歴、そして、最小帯域幅から最大帯域幅までユーザに割当られた帯域幅の履歴のカラムが存在している。また、T 0 4 には保証帯域幅というカラムがあり、図 1 2 で帯域保証サービスを行ったときに記入される。また、同一時点で複数のユーザのネットワーク負荷の増大が判明し、その複数ユーザにつ

いてネットワーク帯域幅を増加させる必要が生じた場合に、図 1 2 で帯域保証サービスを希望したユーザに対しては、帯域保証サービスを希望しないユーザよりも優先してネットワーク帯域幅の割当変更を行う。

以下、VPN の設定として考えられる夫々の場合について説明する。

(1) まず、第 1 の場合について説明する。図 3 のように VPN の実現方式がデータセンタとキャリアとユーザの 3 つの VPN ルータ群で構成されており、データセンタ管理サーバから全ての帯域変更の指示を出すことを特徴とする場合を考える。データセンタの管理サーバは信号線 L 0 1、L 1 0、L 2 0 を介して各 VPN ルータにおけるネットワーク帯域情報をユーザ及びキャリアの各管理サーバ経由でモニタし (1 5 0 1)、各ユーザごとに稼動情報を集計して図 7 の VPN 稼動表 T 0 5 に格納している (1 5 0 2)。データセンタの管理サーバ C 0 は帯域使用率とサービスレベル契約とを比較し (1 5 0 3)、ネットワーク帯域の削減ができないか検討する (1 5 0 4)。もし設定された帯域幅が 3 M b p s で実際の利用帯域幅が 0. 5 M b p s、帯域利用率の閾値が 4 0 % である場合を考えると帯域幅は削減可能であると判断できる。VPN の場合もサーバ割当と同様に全てのユーザの帯域削減処理を行った後に、帯域追加処理を行う。もし削減対象であれば、データセンタの管理サーバは帯域削減指示を信号線 L 0 1、L 1 0、L 2 0 を介してデータセンタ、ユーザ、キャリアの各管理サーバに対して通知する。通知を受けた各管理サーバは管理下の VPN ルータに対して使用している帯域幅を解放するように指示する。帯域幅を解放する順序はユーザ、キャリア、データセンタの順番に行う。帯域幅の解放が終了すると各管理サーバはデータセンタの管理サーバにその旨通知する。管理サーバ C 0 はそれを待って、VLAN 稼動表 T 0 5 を変更し、使用したネットワークの帯域の履歴等の課金に関するパラメータ情報も変更し、ユーザ及びキャリアの管理サーバの VLAN 稼動表 T 0 9、T 1 1 を変更する (1 5 0 5)。

【 0 0 3 7 】

つづいてネットワーク帯域幅を増強する処理に移る。データセンタの管理サーバ C 0 は帯域幅使用情報をサービスレベル条件と比較し、ネットワーク帯域幅を追加する必要があるかを検討する (1 5 0 6)。データセンタ管理サーバ C 0 は

図7のVPN設定表T04を参照してユーザに割当可能な帯域幅があるか調査する(1507)。もし空きのネットワーク帯域がなければ運用管理者に通知し、帯域幅不足の為のサービスレベル未達か契約条件を超えた為のサービスレベル未達か区別して記録される(1508)。例えば、現在のユーザ割当帯域幅が1.5Mbpsで実際の稼働帯域幅が1.2Mbpsでユーザ設定の帯域利用率が40%で空きの帯域幅が1.5Mbpsである場合等、空きのネットワーク帯域が有る場合にはユーザに対するネットワーク割当帯域幅の追加指示を出す(1509)。ネットワーク帯域幅の変更の順番はデータセンタ、キャリア、ユーザの順番に変更を行う。その後、図7のVPN稼働表T05の内容を変更し使用帯域幅の使用履歴等の課金に関するパラメータ情報を変更し、図8のVPN稼働表T09、図9のVPN稼働表T11の帯域幅の使用履歴等の課金に関するパラメータ情報を変更する(1510)。

【0038】

本変更方式の利点は、データセンタ、キャリア、ユーザを通じたVPNのネットワーク帯域を一括制御することで、VPNのネットワーク全体の負荷のバランス及びサーバのネットワーク負荷等を総合的に判断したネットワーク帯域の制御ができる点である。

(2) 図3の構成で、(1)の場合と異なるもう1種類のVPNの設定方法がある。データセンタの管理サーバC0がネットワーク帯域幅の割当判断ルールを信号線L01、L10、L11、L20、L21を介して予めユーザの帯域管理サーバC10及びキャリアの帯域管理サーバC20に設定することを特徴とする方法である。この場合について説明する。データセンタの管理サーバC0は信号線を通じてユーザ、キャリア、データセンタにおけるネットワーク帯域幅の利用状況をそれぞれの管理サーバC10、C20、C0を通じて収集している。この情報は課金において使われる。また、ユーザ、キャリアの各管理サーバはデータセンタ管理サーバから設定されたネットワーク帯域幅に関するVPN設定表(図7の表T04、図8の表T08、図9の表T10)とVPN稼働表(図7のT05、図8のT09、図9のT11)を持っている。各管理サーバはネットワーク帯域利用情報をモニタリングし(1501)、ユーザの場合には稼働情報を集計して図

8のVPN稼働表T09に格納する(1502)。各管理サーバはネットワーク帯域幅利用情報とVPN設定表(図7のT04、図8のT08、図9のT10)を比較した後(1503)、まずサービスレベル契約に照らしてネットワーク帯域を削減できないか検討する(1504)。(1)の場合と同様にもし帯域幅が削減可能であれば、各管理サーバはネットワーク帯域削減を行う。帯域幅を削減する順序は各管理サーバ間で連絡を取り合いながらユーザ、キャリア、データセンタの順番にルータに指示する。その後、削減処理を行ったVPNルータを管理する管理サーバは新たにユーザに割当られた帯域情報を信号線L01、L10、L20を通じてデータセンタ管理サーバに通知する。データセンタの管理サーバは変更を行った各管理サーバからの情報を受け取った後、図7のVPN稼働表T05の帯域幅履歴を変更してユーザの利用した帯域幅の履歴など課金に関するパラメータ情報を変更する(1505)。同時に、図8のユーザのVPN稼働表T09、図9のキャリアのVPN稼働表T11が変更される。次に、ネットワーク帯域追加処理を行う。データセンタ、ユーザ、キャリアの各VPNルータはネットワークの稼働状況とVPN設定表(図7の表T04、図8の表T08、図9の表T10)と比較し、ネットワーク帯域幅を追加する必要があるかを検討する(1506)。(1)の場合と同様に増強する必要がある、各管理サーバの管理しているネットワーク帯域に空きがある場合、各管理サーバは管理下のVPNルータに対して帯域幅追加を行う(1507)。もし空きのネットワーク帯域がなければ運用管理者に通知し、帯域幅不足の為のサービスレベル未達か契約条件を超えた為のサービスレベル未達か区別して記録される(1508)。その後、新たにユーザに割当てられた帯域情報を信号線を通じてデータセンタ管理サーバC0に通知する。(1509)ネットワーク帯域幅の変更の順番は管理サーバ間で連絡を取り合いながらデータセンタ、キャリア、ユーザの順番に変更を行う。データセンタの管理サーバは変更を行ったVPNルータからの情報を受けとった後、図7のVPN稼働表T05の内容を変更する。同時に、ユーザの帯域管理サーバ上にあるVPN稼働表T09、キャリアの帯域管理サーバ上にあるVPN稼働表T11が変更される。最後にユーザの利用した帯域幅の履歴など課金に関するパラメータ情報を変更する(1510)。

本変更方式の利点は、ユーザ、キャリア、データセンタのそれぞれのネットワークで帯域幅使用の監視と割当判断の制御を行うので、制御が早く行える点である。

(3) 図4のようにデータセンタ業者とキャリア業者が同一の場合である。この場合はデータセンタの管理サーバC0はデータセンタとユーザのVPNルータ群を制御対象とすると考えれば良い。第1の場合と同様に、データセンタの管理サーバは信号線L11、L30を介して各VPNルータにおけるネットワーク帯域情報をモニタする。(ユーザの帯域情報は、ユーザの管理サーバ経由でモニタする)(1501)。各ユーザごとに帯域使用率等の稼動情報を集計して図7のVPN稼動表T05に格納している。本場合についてはキャリアの欄は存在しない(1502)。データセンタの管理サーバC0は帯域使用率情報をサービスレベル契約と比較して(1503)、ネットワーク帯域を削減できないか検討する(1504)。もし削減可能であれば、データセンタの管理サーバC0は帯域削減指示を信号線を介してユーザの管理サーバに対して通知する。帯域幅を削減する順序はユーザ、データセンタの順番に行う。通知されたユーザの管理サーバは管理下にあるVPNルータに対し使用している帯域幅を解放するよう指示する。帯域幅の解放が終了するとユーザの管理サーバはデータセンタの管理サーバC0にその旨通知する。データセンタの管理サーバC0はそれを待って、図7のVPN稼動表T05を変更し、ユーザが使用した帯域幅の履歴など課金に関するパラメータ情報を変更する(1505)。つづいてネットワーク帯域幅を増強する処理に移る。データセンタの管理サーバC0は、帯域使用率情報をVPN設定表T04と比較してネットワーク帯域幅を追加する必要があるかを検討する(1506)。増強する必要があるれば、データセンタ管理サーバは図7のVPN設定表T04を参照してユーザに割当可能な帯域幅があるか調査する(1507)。もし空きのネットワーク帯域がなければ運用管理者に通知し、帯域幅不足の為のサービスレベル未達か契約条件を超えた為のサービスレベル未達か区別して記録される(1508)。空きのネットワーク帯域があればユーザの管理サーバに対してネットワーク割当帯域を追加指示を出す。(1509) ネットワーク帯域幅の変更の順番はデータセンタ、ユーザの順番に変更を行う。その後、VPN稼動表T0

5の内容を変更し、課金に関するパラメータ情報を変更する（1510）。

【0039】

以上述べたように帯域を削減する時はユーザ側が先に削減し、増強する場合はデータセンタ側から先に増強する。

【0040】

次に、ストレージネットワークの動的変更について説明する。ストレージネットワークの概要を図5に示す。先にVLAN設定で説明したように負荷分散装置からDBサーバまではユーザは専用のVLANを組んでいる。一方、ユーザに割当てられたDBサーバとストレージネットワークスイッチとストレージのLUNは同じゾーンに属するように制御する。データセンタ管理サーバは図10のストレージネットワーク構成表T06のような構成情報を記録する。

図10の説明を行う。図10には図13のサービスレベル条件入力を元に作成されるユーザ条件設定表T01があり、ストレージネットワークのポートの最小帯域幅及び最大帯域幅、ストレージネットワークスイッチのポートの帯域利用率の閾値のカラム、初期LUNアクセス優先度のユーザがサービスレベル入力画面で設定した条件を保持している。また、ストレージネットワーク構成表T06には、ユーザ条件設定表T01の内容にそって、ストレージネットワークでの帯域幅の最大・最小、SLAで約束した帯域使用率の閾値、割当LUN、LUNアクセス初期優先度、所属DBサーバ、ゾーン所属のポートのカラムがあり、ストレージネットワークの構成が記述される。表T07においてはユーザのストレージネットワークのユーザに割り当てられた帯域幅について、帯域使用率を満たしている時間そしてサービスレベル条件を超えた等の理由で満たせなかった時間の履歴、そして、最小帯域幅から最大帯域幅までユーザに割当られた帯域幅の履歴のカラム、LUNアクセス優先度の履歴のカラムが存在している。

ゾーンの技術については公知である。図5のようにVLANとゾーンを組み合わせることで、たとえば、ユーザAからユーザBが用いるべきストレージのLUNにアクセスを試みることを考える。この時、ストレージs01では図10のストレージネットワーク構成表T06に相当する情報を参照することでユーザBのLUN LU02はゾーンZ02所属でユーザAはゾーンZ01所属なのでアクセ

スが拒否されるというようにユーザのセキュリティが保たれる。

さて、ストレージネットワークの負荷が変動した時のストレージネットワーク部分の処理について考える。データセンタの管理サーバC0は各ゾーンに関する稼働状況を集集し、ストレージネットワーク稼働表T07に格納する。具体的にはデータセンタの管理サーバは信号線L08を介してストレージネットワークの帯域情報をモニタし(2801)、各ユーザごとに稼働情報を集計して図10のストレージネットワーク稼働表T07に格納している(2802)。ストレージネットワークスイッチSW03の使用帯域に関しては図10のストレージネットワーク構成表T06と比較した後(2803)、まずサービスレベル契約に照らしてネットワーク帯域を削減できないか検討する(2804)。ストレージネットワークにおいても、全ユーザに対する削減処理が終わってから増強処理を行う。もし削減可能であれば、管理サーバC0は図10のストレージネットワーク構成表T06のアクセス優先度のカラムや利用帯域幅のカラムの変更を行い、削減対象であるネットワーク帯域削減要求を信号線を介してストレージネットワークスイッチSW03に出す。通知を受けたストレージネットワークスイッチSW03はユーザが使用しているストレージネットワークの帯域幅を削減する(2805)。次に、ストレージのLUNへのアクセス優先度を下げるように信号線を通じストレージネットワークスイッチSW03に通知する。例えば、帯域を減少するときはLUNへのアクセス優先度を予め決められた量だけデクリメントするような指示を出す(2806)。通知を受けたストレージネットワークSW03はストレージのアクセス優先度を下げる。その後、図10のストレージネットワーク稼働表T07のアクセス優先度のカラムや利用帯域幅のカラムの変更を行い、ユーザの利用した帯域幅履歴やアクセス優先度履歴等の課金に関するパラメータ情報を変更する(2807)。

つづいてストレージ資源を増強する処理に移る。データセンタ管理サーバは図10のストレージネットワーク構成表T06と比較し、ストレージネットワークのネットワーク帯域幅を追加する必要があるかを検討する(2808)。増強する必要があるれば、データセンタ管理サーバはユーザ条件設定表T01を参照してユーザに割当可能な帯域幅があるか調査する(2809)。もし空きのネットワー

ク帯域がなければ運用管理者に通知し、帯域幅不足の為のサービスレベル未達か契約条件を超えた為のサービスレベル未達であるか区別して記録される（2810）。空きのストレージネットワーク帯域があれば、データセンタの管理サーバC0は図10のストレージネットワーク構成表T06のアクセス優先度のカラムや利用帯域幅のカラムの変更を行い、ストレージのLUNへのアクセス優先度を上げるように信号線を通じストレージネットワークスイッチSW03に通知する。例えば、帯域を増加するときはLUNへのアクセス優先度を予め決められた量だけインクリメントするような指示を出す。通知を受けたストレージネットワークスイッチSW03はストレージのアクセス優先度を上げる（2811）。次にストレージネットワークスイッチSW03にユーザに対するストレージネットワークの割当帯域の追加指示を出す（2812）。その後、データセンタ管理サーバは図10のストレージネットワーク稼働表T07のアクセス優先度のカラムや利用帯域幅のカラムの変更を行い、ユーザの利用したストレージネットワークの帯域幅の履歴やアクセス優先度の履歴など課金に関するパラメータ情報も変更する（2813）。

このストレージネットワークの帯域幅とアクセス優先度の変更手順を逆にした場合ストレージネットワークにおいてストレージにリクエストが殺到した場合にストレージへのアクセスビジーが生じるので、性能低下が起こる。よって、この変更順序は必然である。

【0041】

ここで、ユーザの負荷が大きくなった時及び負荷が小さくなった時の本特許で述べているユーザ、キャリア、データセンタで構成されるシステム全体の資源割当変更手順に関して図26及び図27にまとめた。

システムの負荷が増大する場合の変更手順を示している図26の構成は、2606から2608までのVPN変更部分、2603から2605までのVLAN変更部分そして2601から2602までのストレージネットワーク変更部分に分けられる。処理の変更順序については、2606から2608のVPN部分、2603から2605のVLAN部分、2601から2602のストレージネットワーク部分の各グループの中においては、順序通りに変更を行えば変更によって

セキュリティの低下やWebサービスが悪化が生じることは無いという意味で必然である。また、ストレージネットワーク、VLAN、VPNグループの順に変更の過程でWebサービスが悪化が生じることは無いという意味で必然である。具体的に例を挙げる。VPNの変更部分の変更順序を守らない場合、例えば、ネットワークの負荷が大きい場合ユーザのネットワーク出口の帯域幅追加の変更をした後にデータセンタ入口の帯域幅追加の変更をする場合を考えると、データセンタへのアクセスが集中することによってデータセンタのネットワークビジーを原因とするWebサービスの品質の低下が起こる。また、VLAN部分の変更順序を守らない場合を考える。例えば、図2においてWebサーバ10をユーザAのネットワークに追加することを考えた場合、LB01、SW01の順にVLANの変更を行うと、データセンタ内の遊休サーバにアクセスできてしまうというようにシステムのセキュリティが守られない可能性が有る。

一方、システムの負荷が減少する場合の変更手順を示している図27の構成は、2701から2703のVPN変更部分、2704から2706までのVLAN変更部分、2707から2708までのストレージネットワーク変更部分の各グループの中においては、順序通りに変更を行えば変更によってセキュリティの低下やWebサービスが悪化が生じることは無いという意味で必然である。また、VPN、VLAN、ストレージネットワークグループの順に変更を行うことでも変更の過程でWebサービスが悪化が生じることは無いという意味で必然である。

VLAN部分の変更順序を守らない場合を考える。例えば、図2においてWebサーバa10をユーザAのネットワークから削減することを考えた場合、SW01、LB01の順にVLANの変更を行うと、データセンタ内の他の遊休サーバ群にアクセスできてしまうというようにシステムのセキュリティが守られない可能性が有る。

本変更に関する変更の方針を以下に記す。

(i) システムの負荷が高い時に変更を行う場合には、深層から表層の向きに変更を行う。

(i i) システムの負荷が低い時に変更を行う場合には、表層から深層の向きに

変更を行う。

【 0 0 4 2 】

最後に本システムの課金について記述する。VPN、VLAN、ストレージネットワークの3つの部分に分けて、夫々の部分で課金したものの総和をユーザに課金する。（キャリアの分もデータセンタがまとめて課金する。）

（ i ） VPN部分について

（単位時間における割当帯域幅の料金×ユーザへの割当時間－帯域条件未達時の基本違約料金×ネットワークのリソース不足による帯域条件未達になった時間）×（重み付け係数） で求める。すなわち、延べ使用時間分の使用料金から罰金を引くという形で課金する。

帯域幅の基本料金はユーザに割り当てられる帯域幅の大きさによって段階的に変化する。

すなわち、割当帯域幅の料金は b を帯域幅と定義し、 b は正規化しているものとして表現する。このとき、

$P(b)$: ユーザに割当てたネットワーク帯域幅 b の場合の単位時間当りの使用料。

$T(b)$: ネットワーク帯域幅 b がユーザに割当てられている時間。

すると、ユーザの延べ使用時間分の課金は

$$\sum_b P(b) \times T(b) \cdots \cdots \text{(数 1)}$$

で割当てられる。 $P(b)$ は b の値による階段関数や比例関数などさまざまな料金設定が考えられる。なお、（重み付け係数）は通常は1であり、図12において帯域保証サービスを選んだ場合に1より大きな値を持つ係数である。

（ i i ） VLAN部分について

（サーバ1台の基本料金×ユーザへの割当台数×ユーザへの割当時間－サービスレベル条件未達時の基本違約金×ユーザへの割当台数×サーバ不足によるサービスレベル条件未達時間）×（重み付け係数）で求める。

ユーザの延べ使用時間分の課金に関して、基本的な概念は（i）の（数1）式と同様である。なお、（重み付け係数）は通常は1であり、図12においてセキュリティオプションを選んだ場合に1より大きな値を持つ係数である。サーバの使

用料はWeb、AP、DB層毎に計算した合計になる。上記(i)のVPN部分と同様に、サーバの基本料金はユーザに割当てられたサーバの台数により段階的に変化する。

(iii) ストレージネットワーク部分について

(単位時間における割当帯域幅の基本料金) × (ユーザへの割当時間 + 単位時間のアクセス優先度に応じた基本料金) × (ユーザへのアクセス優先度の設定時間 - サービスレベル条件未達時の基本違約金) × (ネットワークのリソース不足による帯域条件未達になった時間) で求める。

ユーザの延べ使用時間分の課金に関して、基本的な概念は(i)の(数1)式と同様である。帯域幅の基本料金はユーザに割り当てられる帯域幅の大きさによって段階的に変化する。

[2] 第2の実施形態

続いてパーティション機能仮想計算機機能PRMFを備えた高多重SMPサーバを用いてデータセンタを構成する場合の実施形態を説明する。

まず、実施形態を説明する主な図の説明をする。図17はLPARサーバを用いた場合のデータセンタの内部構造を示している。図18、図19は、ユーザ企業Aが本データセンタと使用条件契約を結ぶときの入力画面の一例を示している。

図20はVLANに関する管理サーバの持つ情報の一覧を示している。図21はVPNに関する管理サーバの持つ情報の一覧を示している。図22はストレージネットワークに関する管理サーバの持つ情報の一覧を示している。図23は実施形態で用いるパケットの一例を示す。図24は、契約を結んだユーザに対してサーバのCPU利用率が割り当てる手順を示したものである。図25はユーザに割り当てられるサーバのCPU利用率が動的に増大・減少する時の手順を示したものである。

さて、実施形態の説明に入る。データセンタとユーザの接続図は図1に同じである。

【0043】

図17は、webサーバ、APサーバ、DBサーバとして仮想計算機機能PRMFを備えたサーバをおのおの1台ずつ接続した場合を示している。APサーバ

P 0 2、DBサーバP 0 3の内部構成はwebサーバP 0 1と同様であり記述は省略することにする。

【0 0 4 4】

図1 8、1 9は、サービスレベル契約条件入力画面の一例である。本例では、ユーザ企業Aのために、webサーバ、APサーバ、DBサーバいずれも必ずPRMF機能によるCPU割当てが5 0 %以上となるよう制御する契約である。

【0 0 4 5】

図1 7に戻ると、webサーバP 0 1は、制御ユニットCL 1 0 0、LPAR制御レジスタCL 1 0 1、CPU群CP 0 1およびCP 0 2、メモリM 0 1、ネットワークアダプタt 1 0 0、y 1 0 0から構成される。LPARとはLogical PARTition（論理資源分割）の略であり、LPAR制御レジスタCL 1 0 1は、各OSに与える資源の分割方法を保持している。

【0 0 4 6】

さて、LPAR#は、各パーティションに統一的に与える識別子である。ネットワークアダプタは複数のユーザを1枚で賄う。ネットワークアダプタアドレスは、後述するが制御プログラムP 1 0により、図1 9のサービスレベル条件入力画面で各ユーザが入力するアドレスと一致するように設定される。ここで、VLANタギングの技術により、1つのポートに対して複数のVLANを設定することができる。また、1つのネットワークアダプタに複数のアドレスを設定することもできる。図1 9により、ユーザAはWebサーバのアドレスをa 1 0 0とし、APサーバ、DBサーバのアドレスをそれぞれa 2 0 0、a 3 0 0とする。同様にユーザBにはWebサーバのアドレスb 1 0 0が割当てっており、APサーバ、DBサーバにはそれぞれb 2 0 0、b 3 0 0が割り当てられるとする。ここで、入ってきたユーザ要求のパケットは、対応するLPARのOS上のプログラムに引き渡される。CPU割当て%欄は各LPARに属するOSおよびその上のプログラムをどのような割合でCPU上で動作させるかを示す。制御ユニットCL 1 0 0が本情報を参照して、LPARの動作割合を制御する。

【0 0 4 7】

本実施例ではLPARとデータセンタ管理サーバC 0の持つユーザ識別子を一

意に対応させる。PRMFの制御を行うこととサーバに接続されているスイッチにVLANを設定することにより、異なるユーザ間では資源が共有されないので、ユーザ間のセキュリティを保つことができる。また、ユーザからデータセンタまではVLANタギングによってパケットに与えられたVLANタグが示すVLANにのみ通信が許される。以上により、ユーザからデータセンタまでのセキュリティが保たれる。

【 0 0 4 8 】

第1の実施形態と同様、ユーザ要求がクライアントa0→webサーバa100→APサーバa200→DBサーバa300→APサーバa200→webサーバa100→クライアントa0と伝わる場合を考える。クライアントa0は図23(1)のパケット2300を生成する。図1のVPNルータA0によりパケット2301が生成され、VPNルータD0によりパケット2302が生成されるのは第1の実施形態と同じである。

【 0 0 4 9 】

パケット2302は信号線L0を介してアドレスa100を持つネットワークアダプタt100に渡され、LPAR#0上のアプリケーションプログラムに渡される。すなわちユーザAのアプリケーションプログラムである。本プログラムはあて先a200を持つパケット2304を生成し、以下同様にAPサーバP02上のA社のアプリケーションプログラム、DBサーバP03上のA社のアプリケーションプログラムに渡される。ここで、WebサーバP01のネットワークアダプタt100上にはアドレスa100、b100があり、各々LPAR#0、1に対応している。(図示していないが、APサーバP02内にもネットワークアダプタt200上のアドレスa200、b200があり、Webサーバと同様に各々LPAR#0、1に対応している。またLPAR#0、1は各々ユーザA、Bに対応している。DBサーバP03においても同様である。)同様にしてDBサーバP03からAPサーバP02、webサーバP01、クライアントa0への返答も正しくA社に割り当てられたLPAR上のアプリケーションプログラムにより実施される。第1の実施形態と同様なので詳しくは説明しないが、上記の動作により図23のパケット2306～2309が順次生成される。ここで

、もしA社のクライアントがB社のパーティションにアクセスしようとした場合、図20のVLAN構成表T22により、ユーザAとユーザBとで属しているVLANが異なるのでアクセスは拒否されて、ユーザ毎のセキュリティは守られる。さて、複数のユーザがいる場合であって、各々のユーザに対して1枚ずつネットワークアダプタを与える場合がVLAN部分の変形例として考えられる。この場合は、各ユーザのネットワークアダプタを通じ、ネットワークスイッチのポートに関してユーザ毎にVLANを組むことでセキュリティが守られる。

【0050】

図20はサーバ構成及びVLAN構成について管理サーバC0が持つ情報を示した図である。T22はVLAN構成表であり、サーバのカラム、ネットワークスイッチのカラム、アドレスのカラム、LPARのカラムを所持し、複数のネットワークスイッチにまたがってもユーザ毎に1つのVLANに属するような設定を実現する。表T21はユーザ条件設定表であり、ユーザがサービスレベル条件入力画面で入力した条件のうち各パーティションへのCPU割当率の上限や下限、ユーザと契約したCPUの使用率の閾値のカラムの内容を所持している。さらに、図20の表T23はサーバ及びVLAN稼働表であり、割当LPARやCPU割当率の履歴、割当られたCPUの稼働率の履歴のカラムに情報が入力される。最後にCPU割当表T24は現在各ユーザへ割当てられたCPU割当率のカラムを情報として持つ。この場合、A社に対してはwebサーバ、APサーバ、DBサーバのいずれにおいてもLPAR内部のCPUの稼働率が50%を超えないようにLPARのCPU割当て率を20%以上70%以下の範囲変化させる契約となっている。

制御プログラムP10は信号線L01～L08から得たモニタリング結果とユーザ条件設定表図20の表T21を照合し、現在の資源割当てがサービスレベル契約を満たしているかを調べ、その結果を図20のサーバ及びVLAN稼働表T23のCPU利用率履歴のカラムに規格化して格納する。たとえばユーザ#0に対応するLPAR内部のCPU使用率履歴を記録する。そのためにどのユーザにどれだけCPU割当てを設定しているかを示すCPU割当て表T24が保持されている。CPU割当表T24は各webサーバ、APサーバ、DBサーバ内のLP

AR制御レジスタ群のCPU割当て%欄と同じの内容を保持している。サーバ及びVLAN稼働表表T23の課金に関するパラメータ情報欄の操作は第1の実施形態と同様である。

【0051】

上記制御を行うために、制御プログラムP10が最初に資源を分割する手順を図24を用いて説明する。

【0052】

最初に図18、19のサービスレベル条件入力画面に示される情報を入力し、ユーザ条件設定表T21を作成する(2401)。つづいてその情報のうち最小・最大帯域幅、帯域使用率に関する情報に沿ってデータセンタの管理サーバ、ユーザの帯域管理サーバ、キャリアの帯域管理サーバにVPN設定表を作成する。また、最小・最大帯域幅、帯域使用率に関する情報信号線L0を介してユーザ、キャリア、データセンタの各VPNルータに設定する(2402)。

【0053】

さらに図19のサービスレベル条件入力画面に示される情報を入力し、図20におけるユーザ条件設定表T21のCPU割当て率の上限・下限のカラム、最大・最小帯域幅のカラム、ユーザ使用の帯域利用率のカラムおよびVLAN構成表T22中のネットワークアダプタのカラムを作成する(2403)。

【0054】

続いて図20のユーザ条件設定表T21を参照してユーザAに最低20%、ユーザBに最低20%のCPU割当てを行うべきことを検出すると、CPU割当て管理表T24とVLAN構成表T22中のCPU割当てのカラムを作成する(2404)。さらに信号線L01~L08を介して図17中のサーバP01、P02、P03内のLPAR制御レジスタ群にVLAN構成表T12の内容を設定する(2405)。その後、サーバに繋がる後段のポート及び前段のポートをVLAN構成表T22のport#のカラムに記述し、各ネットワークスイッチSW10~12にVLAN設定指示を出す(2406)。続いてネットワーク及びストレージネットワークの帯域幅を確保し、VPN設定表T25の帯域幅のカラム及びストレージネットワーク構成表T27の帯域幅のカラムに記述し、各VPNルータ及び

ネットワークスイッチ SW 1 3 に帯域幅設定指示を出す (2 4 0 7) 。

【 0 0 5 5 】

さらに、ユーザ条件設定表 T 2 1 に基づき、図 2 0 のサーバ及び V L A N 稼働表 T 2 3、図 2 1 の V P N 稼働表 T 2 6、図 2 2 のストレージネットワーク稼働表 T 2 8 を作成する (2 4 0 8) 。具体的には、ユーザに対する C P U 稼働率履歴やネットワーク帯域使用率履歴を記録する欄を作成する。

【 0 0 5 6 】

以上により資源分割制御に必要な情報が生成され、V P N ルータ r 0 1 や S W 1 0 ～ S W 1 3、サーバ P 0 1、P 0 2、P 0 3 に設定され、正しく資源分割された状態でシステムが動作開始できる。

【 0 0 5 7 】

続いて以下に、制御プログラム P 1 0 が負荷変動時にパーティション割当てを変更する手順を図 2 5 を用いて説明する。

【 0 0 5 8 】

稼働情報収集 (2 5 0 1)、稼働情報集計 (2 5 0 2)、サービスレベル契約との比較 (2 5 0 3) は第 1 の実施形態と同様である。その後 C P U 割当て率を削減可能か検討し (2 5 0 4)、削減可能であれば該当するサーバの L P A R 制御レジスタ群の内容を変更するよう指示する。削減可能かどうかの判断方法は第 1 の実施形態と同様である。変更終了を待った後、課金に関するパラメータを変更する (2 5 0 5)。本例の場合、割当て CPU 使用率と割り当てた時間の履歴を記録している。課金計算では 1 例として、w e b サーバ、A P サーバ、D B サーバそれぞれについて単位時間あたりの使用単価を決めておき、単価 × CPU 使用率を合計して課金する方法も考えられる。

【 0 0 5 9 】

つづいて C P U 割当て率を増強すべきか検討し (2 5 0 6)、増強する必要がある場合は、該当するサーバに設定している C P U 割当て率を増強できないか調べる (2 5 0 7)。割当てできない場合は運用管理者に通知し、C P U 能力不足の為のサービスレベル未達か契約条件を超えた為のサービスレベル未達か区別して記録される (2 5 0 8)。該当するサーバの L P A R 制御レジスタ群の内容を変更す

るよう指示し、変更終了を待った後、課金に関するパラメータ情報を変更する（2509）。

VPNやストレージネットワークにおいても稼動状態によって変更が行われるが、変更方法については第1の実施形態と全く同じであるので割愛する。

【0060】

最後に課金についてであるが、VPNとストレージネットワークについての課金は第1の実施形態と全く同じである。VLAN部分についての課金は以下のように行う。

$(\text{単位時間当りのCPU割当率に関する基本料金} \times \text{ユーザへのCPU割当率} \times \text{ユーザへの割当時間} - \text{単位時間当りのサービスレベル条件未達時のCPU割当率の基本違約金} \times \text{ユーザへのCPU割当率} \times \text{CPUリソース不足によるサービスレベル条件未達時間}) \times (\text{重み付け係数})$

ここで、（重み付け係数）は通常1であり、図18においてセキュリティサービスを選んだ場合に1より大きな値をとる係数である。

〔3〕第1の実施形態の変形例

（a）第1の実施形態の変形例1として、図2のデータセンタにおいて、ユーザ毎の専用VLAN所属のネットワークスイッチ（SW01からSW02）のポートについてポートの帯域に関する帯域幅の割当の動的変更及び帯域幅保証を行うような場合が考えられる。このような場合としては、ユーザのVLANのトラフィックとインターネットからのアクセスなどの他のトラフィックがスイッチの同じポートを共有するような場合が考えられる。まず、VPN部分やストレージネットワーク部分における稼動状況による資源割当の動的な変更方法・課金方法については、実施形態1の通常の場合と全く同じなので割愛する。

図29は管理サーバC0が持つVLAN部分の情報について記した図である。負荷分散装置のアドレス対応表T00に関しては第1の実施形態の通常の場合と同じ情報である。さて、この変形例で管理サーバC0が持つVLAN部分の情報として特徴的な点を、図29を参照して説明する。まず、図6のユーザ条件設定表T01に負荷分散装置LB01及びネットワークスイッチSW01、SW02の最大・最小割当帯域幅、帯域使用率の閾値のカラムを追加した表T31がある。

また、図 6 の V L A N 構成表 T 0 2 に L B 0 1 及びネットワークスイッチ S W 0 1、S W 0 2 の最大帯域幅・最小帯域幅、帯域利用率の閾値のカラムを追加した V L A N 構成表 T 3 2、図 6 のサーバ及び V L A N 稼働表 T 0 3 に L B 0 1 及びネットワークスイッチ S W 0 1、S W 0 2 の帯域幅利用履歴のカラムが追加された V L A N 構成表 T 3 3 がある。

まず、システム立上げ時にサーバ割当を変更する方法を述べる。ユーザに専用の V L A N を設定する手順は、ネットワークスイッチのポートを V L A N に割当て るまでは、第 1 の実施形態の通常の場合とまったく同じであるが、ポートをユーザの V L A N に割当てた後、図 1 2、図 1 3 のサービスレベル条件入力画面で設定した内容にそって作成された図 2 9 のユーザ条件設定表 T 0 1 の最大帯域幅、最小帯域幅、帯域利用率のカラムの情報に従って先にユーザ専用の V L A N に割当てられたそれぞれのポートに対して V P N の帯域割当方法と全く同じ方法で帯域幅を割当てる。V L A N 所属のポートに帯域幅を割当てた後、V P N の設定やストレージネットワークの設定を行い、資源分割を行う。

次に、図 2 9 の制御プログラム P 1 0 が負荷増大時にサーバ割当を変更する手順を説明する。図 1 6 のフローチャートにおいて、1 6 0 3 までのステップすなわち稼働情報収集からサービスレベルとの比較までのステップは通常の実施形態と同じである。図 2 9 のユーザ条件設定表 T 0 1 の帯域幅のカラムと比較した後にサービスレベル契約に照らしてネットワーク帯域を削減できるか否かを検討し、データセンタの管理サーバは帯域削減対象であるポートの帯域幅に対して帯域幅削減要求を出す。帯域幅変更方法は図 2 において L B 0 1 のポート、S W 0 1 のポート、S W 0 2 のポートである。（ユーザ A であれば、p 0 0 1、p 1 0 1、p 2 0 1、p 3 0 1、p 4 0 1 の順に帯域幅の変更を行う。）その後、サーバを接続しているポート対する V L A N の変更、サーバの削減処理、サーバの追加処理など図 1 6 の 1 6 0 4 から 1 6 1 2 の項までのステップは通常の実施形態と同じである。サーバを追加し、サーバを接続しているポート対する V L A N の変更が行われたあと、図 2 9 のユーザ条件設定表 T 0 1 の帯域幅のカラムと比較した後にサービスレベル契約に照らしてネットワーク帯域を追加できるか否かを検討し、データセンタの管理サーバは帯域追加対象であるポートの帯域幅に対して

帯域幅追加要求を出す。帯域幅変更方法は図 2 において SW 0 2 のポート、SW 0 1 のポート、LB 0 1 のポートの順番である。（ユーザ A であれば、p 5 0 1、p 4 0 1、p 3 0 1、p 2 0 1、p 1 0 1、p 0 0 1 の順に帯域幅の変更を行う。）その後の処理は図 1 6 のフローチャートと全く同じである。

最後に VLAN 部分の課金について述べる。この変形例に適する課金は、第 1 の実施形態の VLAN 部分の課金に帯域利用の項を追加したもので以下のように表現できる。

【 0 0 6 1 】

（単位時間当りのサーバ 1 台の基本料金×ユーザへの割当台数×ユーザへの割当時間 — 単位時間当りのサービスレベル条件未達時の基本違約金×ユーザへの割当台数×サーバ不足によるサービスレベル条件未達時間）×（重み付け係数 1）+

（単位時間当りのネットワークスイッチのポートにおける帯域幅の基本料金×ユーザへの割当時間 — ネットワークスイッチのポートにおける帯域条件未達時の基本違約金×ネットワークリソース不足による帯域条件未達時間）×（重み付け係数 2）

ここで（重み付け係数 1）は通常は 1 で図 1 2 においてセキュリティサービスを選んだ場合に 1 を超える値をとる係数である。（重み付け係数 2）通常は 1 で図 1 2 において帯域保証サービスを選んだ場合に 1 を超える値をとる係数である。基本的な考え方は第 1 の実施形態の通常の場合と同様である。

ネットワークスイッチのポートにおける帯域幅の基本料金はユーザに段階的に割り当てられる帯域幅の大きさによって段階的に変化する。

（b）第 1 の実施形態の変形例 2 として、図 3 0 のようにユーザ毎に専用の VPN ルータ、負荷分散装置のポートを持つ構成も可能である。本実施例では VLAN タギングの技術によってではなく、ユーザ専用割り当てられた VPN ルータ、負荷分散装置のポートに設定される VLAN ID によって各ユーザが区別される設定になっている。一連の動作は第 1 の実施形態の場合と同様である。

（c）第 1 の実施形態の変形例 3 のサーバおよび VLAN の割当て変更のフローを図 3 2 に示す。図 2 のデータセンタにおいて、サーバをユーザに割り当てる時

に割当てられる該サーバの電源を入れ、サーバをユーザから外すときにユーザ割当てを外れた該サーバの電源を切るという電源制御を行う場合を考える。この場合は、ユーザにサーバ割当て変更を行うフローを示した図 1 6 に関して、ユーザにサーバを割当てる直前に割当てたサーバの電源を入れるステップ(3 2 0 7)とユーザからサーバの割当てを外した後にサーバの電源を落とすステップ(3 2 1 2)を追加した図 3 2 に従って動作を行う。追加した 2 つのステップ以外の一連の動作は第 1 の実施形態の場合と同様である。

〔 4 〕 第 2 の実施形態の変形例

第 2 の実施形態の変形例として、図 1 7 のデータセンタにおいて、ユーザ毎の専用 V L A N 所属のネットワークスイッチ (S W 0 0 から S W 0 2) のポートについてポートの帯域に関する帯域幅の割当ての動的変更及び帯域幅保証を行うような場合について述べる。まず、 V P N 部分やストレージネットワーク部分における稼動状況による資源割当ての動的な変更方法・課金方法については、実施形態 1 の通常の場合と全く同じなので割愛する。

図 3 1 は管理サーバ C 0 が持つ V L A N 部分の情報について記した図である。 C P U 割当て表 T 2 4 に関しては第 2 の実施形態の通常の場合と同じ情報である。さて、図 3 1 には図 2 0 のユーザ条件設定表 T 2 1 に S W 1 0 及びネットワークスイッチ S W 1 1、 S W 1 2 の最大帯域幅・最小帯域幅、帯域利用率のカラムを追加したユーザ条件設定表 T 4 1、 V L A N 構成表 T 2 2 に S W 1 0 及びネットワークスイッチ S W 1 1、 S W 1 2 の最大帯域幅・最小帯域幅、帯域利用率のカラムの情報を追加した V L A N 構成表 T 4 2、図 6 のサーバ及び V L A N 稼動表 T 2 3 に S W 1 0 及びネットワークスイッチ S W 1 1、 S W 1 2 の帯域幅利用履歴のカラムが追加された V L A N 構成表 T 4 3 がある。

まず、システム立上げ時にサーバ割当てを変更する方法を述べる。ユーザに専用の V L A N を設定する手順は、ネットワークスイッチのポートを V L A N に割当てるまでは、第 2 の実施形態の通常の場合とまったく同じであるが、ポートをユーザの V L A N に割当てた後、図 1 8、図 1 9 のサービスレベル条件入力画面で設定した内容にそって作成された図 3 1 のユーザ条件設定表 T 4 1 の最大帯域幅、最小帯域幅、帯域利用率のカラムの情報に従って先にユーザ専用の V L A N に割

当てられたそれぞれのポートに対してVPNの帯域割当方法と全く同じ方法で帯域幅を割当てる。VLAN所属のポートに帯域幅を割当てた後、VPNの設定やストレージネットワークの設定を行い、資源分割を行う。

次に、図31の制御プログラムP10が負荷増大時にサーバ割当を変更する手順を説明する。図25のフローチャートにおいて、2503までのステップすなわち稼働情報収集からサービスレベルとの比較までのステップは通常の実施形態と同じである。図31のユーザ条件設定表T21の帯域幅のカラムと比較した後にサービスレベル契約に照らしてネットワーク帯域を削減できるか否かを検討し、データセンタの管理サーバは帯域削減対象であるポートの帯域幅に対して帯域幅削減要求を出す。帯域幅変更方法は図17においてSW10のポート、SW11のポート、SW12のポートである。（ユーザAであれば、p001、p101、p201、p301、p401の順に帯域幅の変更を行う。）その後、CPU割当率の削減処理、CPU割当率の追加処理など図25の2504から2506の項までのステップは通常の実施形態の場合と同じである。CPU割当を追加したあと、図31のユーザ条件設定表T41の帯域幅のカラムと比較した後にサービスレベル契約に照らしてネットワーク帯域を追加できるか否かを検討し、データセンタの管理サーバは帯域追加対象であるポートの帯域幅に対して帯域幅追加要求を出す。帯域幅変更方法は図17においてSW12のポート、SW11のポート、SW10のポートの順番である。（例えばユーザAであれば、p501、p401、p301、p201、p101、p001の順に帯域幅の変更を行う。）その後の処理は図25のフローチャートと全く同様に考えて、サーバ及びVLAN稼働表T43の帯域幅の使用履歴のカラムを変更し、課金に関するパラメータを変更する。

最後にVLAN部分の課金について述べる。この変形例の課金法は、第1の実施形態のVLAN部分の課金に帯域利用の項を追加したもので以下のように表現できる。

【0062】

（単位時間当りのCPU割当率に関する基本料金×ユーザへのCPU割当率×ユーザへの割当時間 — 単位時間当りのサービスレベル条件未達時の基本違約

金×ユーザへのCPU割当率×CPUリソース不足によるサービスレベル条件未達時間) × (重み付け係数1) + (単位時間当りのネットワークスイッチのポートにおける帯域幅の基本料金×ユーザへの割当時間 - ネットワークスイッチのポートにおける帯域条件未達時の基本違約金×ネットワークのリソース不足によるサービスレベル未達時間) × (重み付け係数2)

(重み付け係数1) は通常は1で図18においてセキュリティサービスを選んだ場合に1を超える値をとる係数である。(重み付け係数2) 通常は1で図18において帯域保証サービスを選んだ場合に1を超える値をとる係数である。ここでも、基本的な考え方は第1の実施形態の通常の場合と同様である。

ネットワークスイッチのポートにおける帯域幅の基本料金はユーザに段階的に割り当てられる帯域幅の大きさによって段階的に課金される。

【0063】

【発明の効果】

以上述べたように、本発明ではユーザ企業ごとにネットワーク構成設定表を与え、それに基づきネットワーク帯域幅、計算資源を与えるとともに、ネットワーク及び計算機の稼動状況のモニタ結果に基づき自動的にユーザ毎にサービスレベル契約と比較してネットワーク資源、計算機資源の量を増減できる。これにより、ユーザ企業側で予測できない急速な負荷変動に対してもリアルタイムに計算資源の割当てを変更可能である。また、ユーザ企業のサーバを独立したVLANにいれ、サーバ割当に応じてVLANの構成を動的に変えることにより、各ユーザのセキュリティを保持することを可能にする。さらに、データセンタのネットワーク負荷増大にはネットワーク帯域幅の動的設定変更で対応し、ユーザは必要な処理を遅延無く実行することができる。

【0064】

また、ストレージ資源を全計算機で共有する場合に計算機資源の割当てを変更しても、ユーザ毎に設定しているVLAN及びストレージネットワークの構成に基づきアクセス権限チェックを行っているため、ユーザ間セキュリティを維持することができる。

【図面の簡単な説明】

【図1】

インターネットを介して接続されるデータセンタとユーザの例である。

【図2】

データセンタの構成の例である。

【図3】

ユーザからキャリアを通じてデータセンタまで組んだVPNの例1である。

【図4】

ユーザからキャリアを通じてデータセンタまで組んだVPNの例2である。

【図5】

図2のデータセンタにおけるストレージネットワーク構成の例である。

【図6】

図2のデータセンタの管理サーバが保持しているVLANに関する情報の一覧である。

【図7】

図2のデータセンタの管理サーバが保持しているVPNに関する情報の一覧である。

【図8】

ユーザの帯域管理サーバが保持しているVPNに関する情報の一覧である。

【図9】

キャリアの帯域管理サーバが保持しているVPNに関する情報の一覧である。

【図10】

図2のデータセンタの管理サーバが保持しているストレージネットワークに関する情報の一覧である。

【図11】

ユーザからデータセンタ内部で処理されるパケットの一覧である。

【図12】

サービスレベル条件入力画面（オプション選択画面）である。

【図13】

サービスレベル条件入力画面（ユーザ条件の詳細を設定）である。

【図 1 4】

図 2 のデータセンタのサーバ及び V L A N、V P N に関する初期割当のフローチャートである。

【図 1 5】

ユーザに対するネットワーク帯域幅の割当変更のフローチャートである。

【図 1 6】

ユーザに対するサーバ及び V L A N の割当変更のフローチャートである。

【図 1 7】

L P A R サーバを用いて構成されたデータセンタの構成の一例である。

【図 1 8】

サービスレベル条件入力画面（オプション選択画面）である。

【図 1 9】

サービスレベル条件入力画面（ユーザ条件の詳細を設定）である。

【図 2 0】

図 1 7 のデータセンタの管理サーバが保持している V L A N に関する情報の一覧である。

【図 2 1】

図 1 7 のデータセンタの管理サーバが保持している V P N に関する情報の一覧である。

【図 2 2】

図 1 7 のデータセンタの管理サーバが保持しているストレージネットワークに関する情報の一覧である。

【図 2 3】

図 1 7 のデータセンタ内部において処理されるパケット一覧である。

【図 2 4】

図 1 7 のデータセンタにおける L P A R 及び V L A N、V P N に関する初期割当のフローチャートである。

【図 2 5】

ユーザに対する C P U 割当率の割当変更のフローチャートである。

【図 2 6】

負荷が増えた場合の V P N、V L A N、ストレージネットワークの各要素に関する変更手順である。

【図 2 7】

負荷が減った場合の V P N、V L A N、ストレージネットワークの各要素に関する変更手順である。

【図 2 8】

ユーザに対するストレージネットワークでの割当変更のフローチャートである。

【図 2 9】

ポートの帯域制御機能を持つネットワークスイッチを持つ場合における図2のデータセンタ管理サーバが持つ V L A N 関連の情報である。

【図 3 0】

V L A N タギングを用いずにユーザ専用の V P N ルータと V L A N を組み合わせることでセキュリティを確保した例である。

【図 3 1】

ポートの帯域制御機能を持つネットワークスイッチを持つ場合における図 1 7 のデータセンタ管理サーバが持つ V L A N 関連の情報である。

【図 3 2】

電源制御を伴うサーバ及び V L A N の割当変更のフローチャートである。

【符号の説明】

D 0 . . . V P N ルータ

C 0 . . . データセンタの管理サーバ

L B 0 1 . . . 負荷分散装置

S W 0 1、S W 0 2 . . . L A N スイッチ

S W 0 3 . . . ストレージネットワークスイッチ

a 1 0、b 1 0、c 1 0 . . . W e b サーバ

a 2 0、b 2 0、c 2 0 . . . A P サーバ

a 3 0、b 3 0、c 3 0 . . . D B サーバ

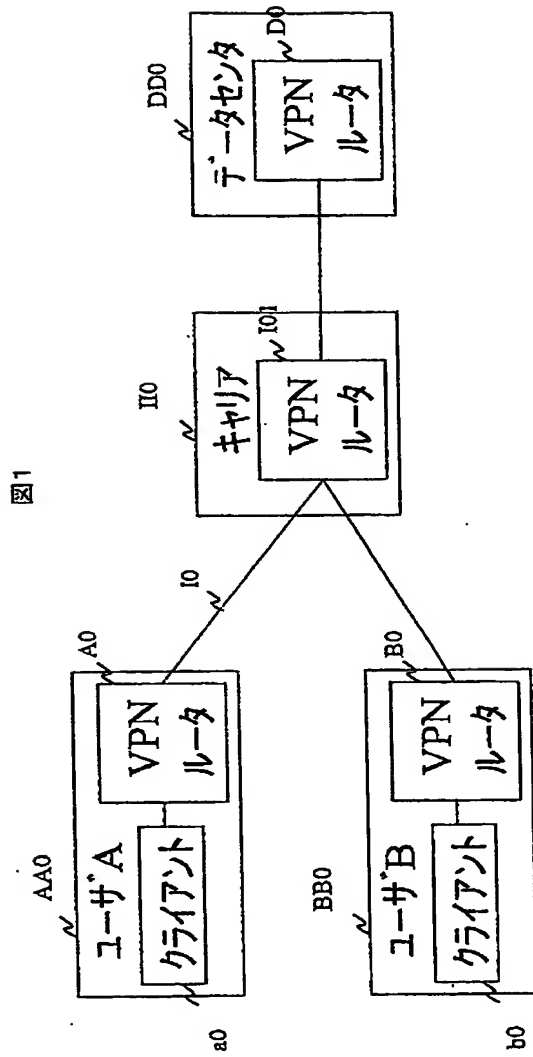
s 0 1 . . . ストレージ

T 0 1 . . . ユーザ条件設定表

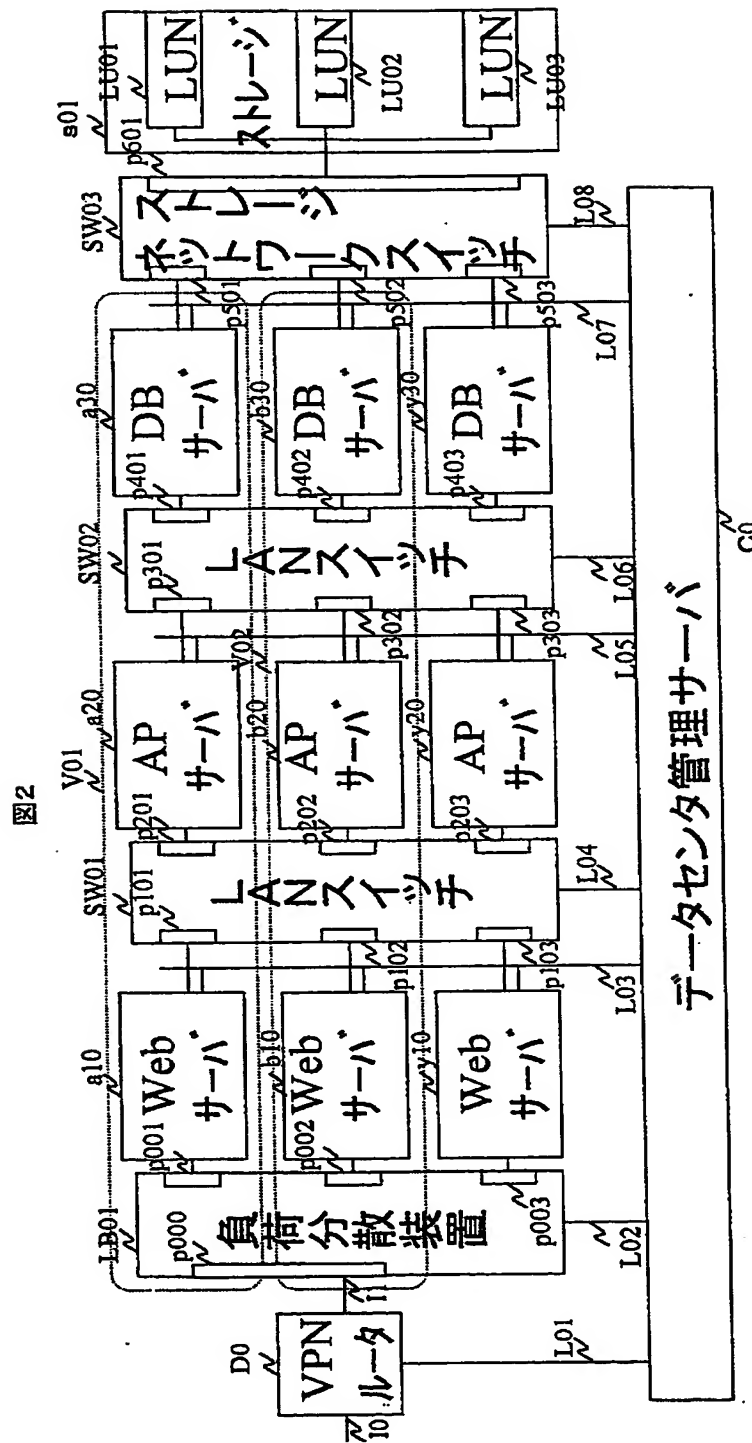
T 0 2 . . . V L A N 構成表。

【書類名】 図面

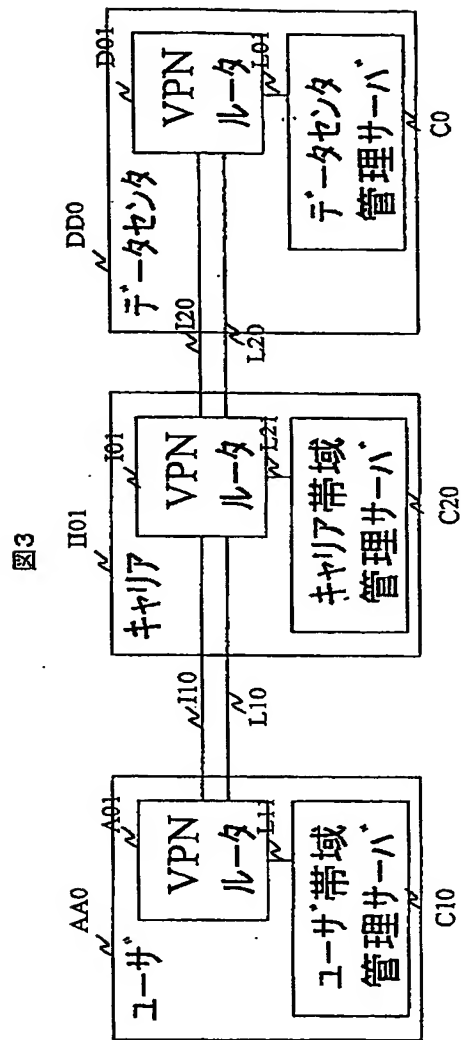
【図 1】



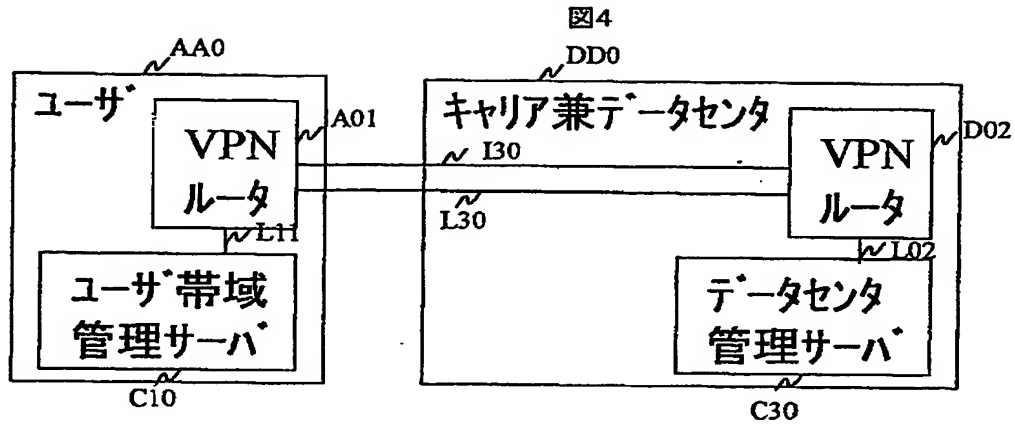
【図2】



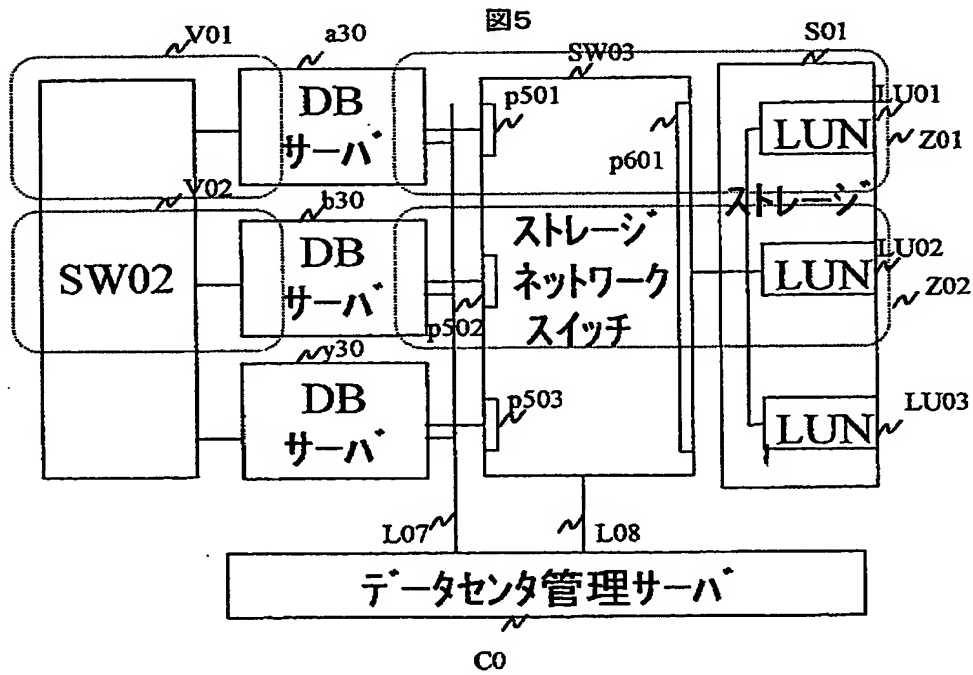
【図 3】



【図4】

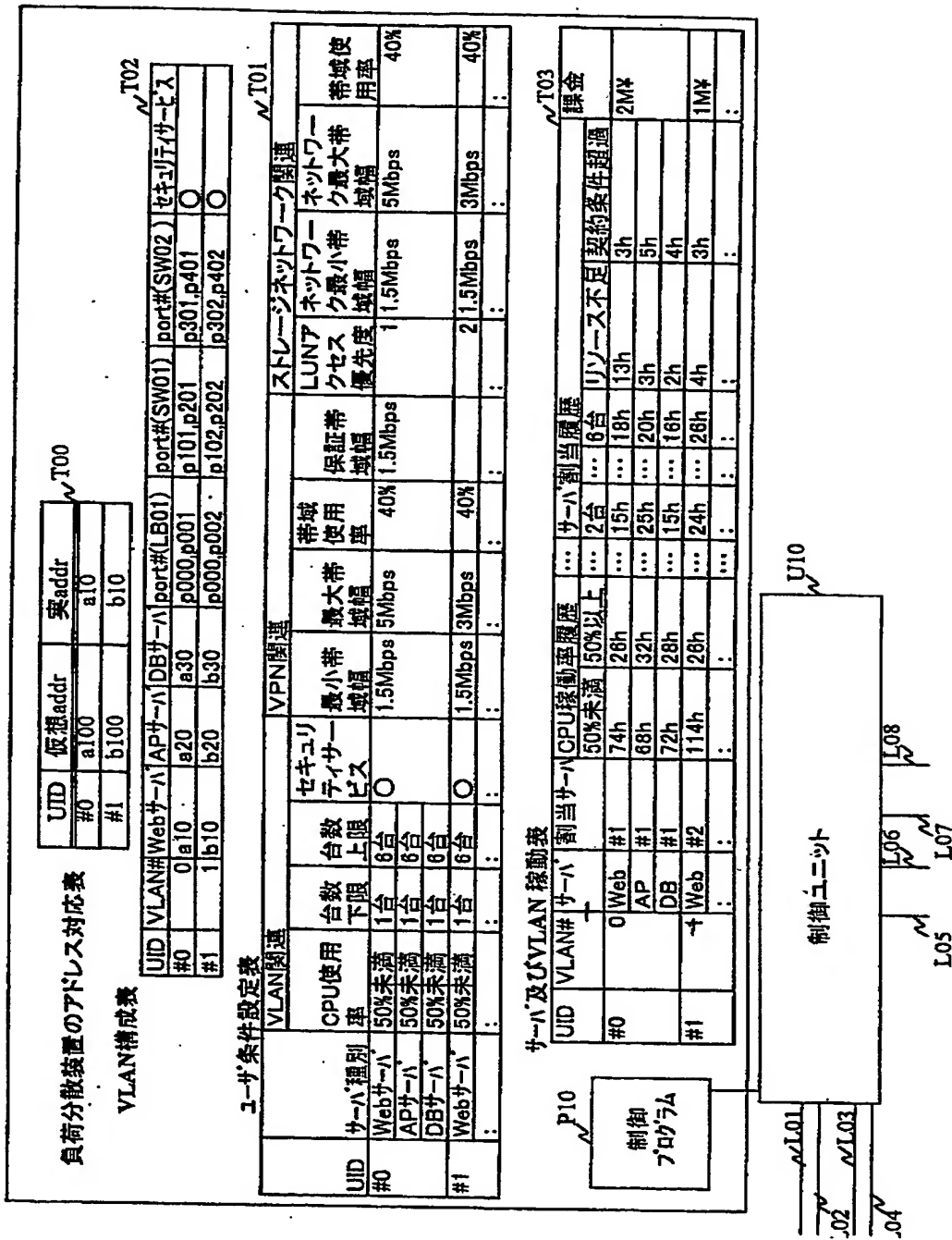


【図5】

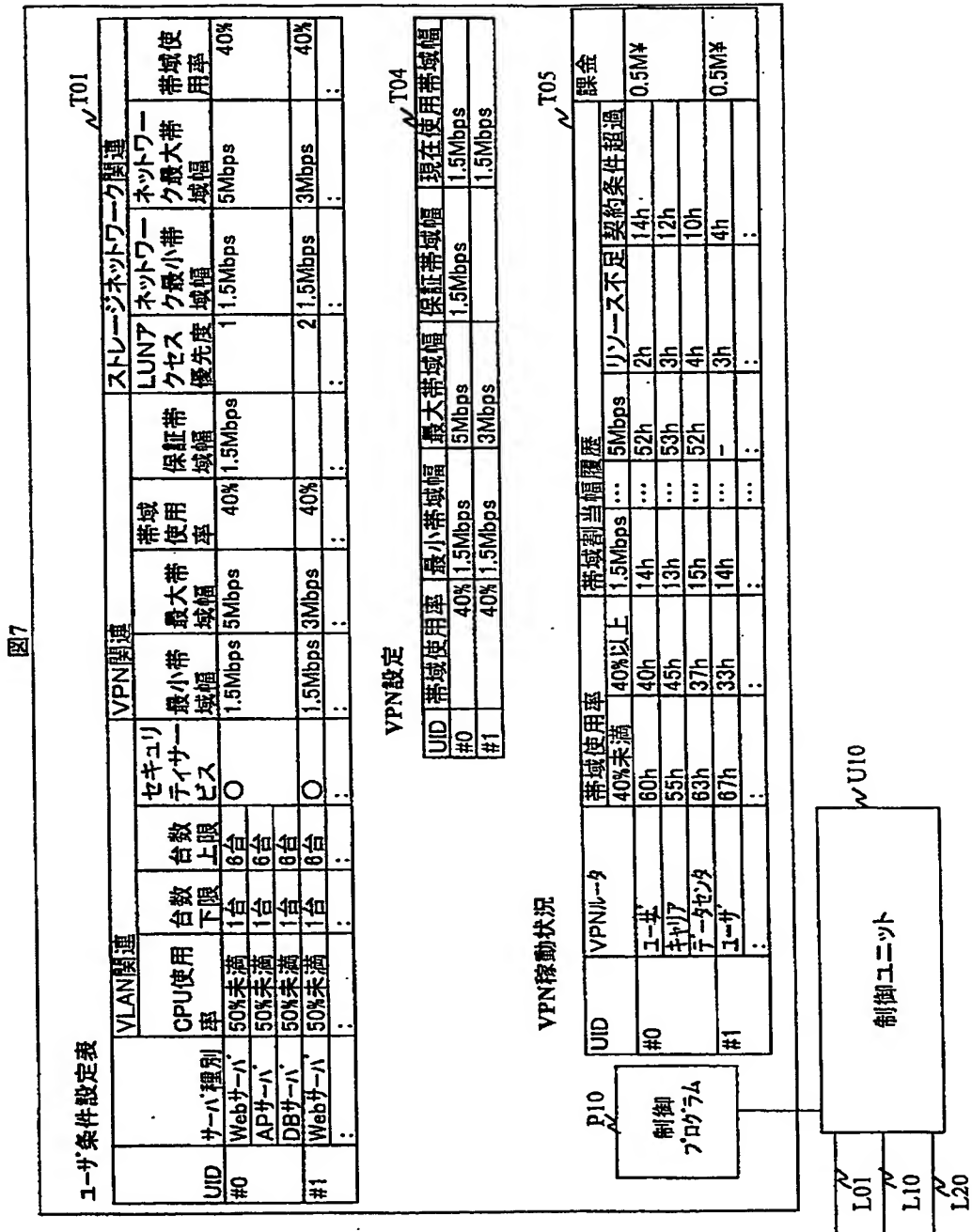


【図 6】

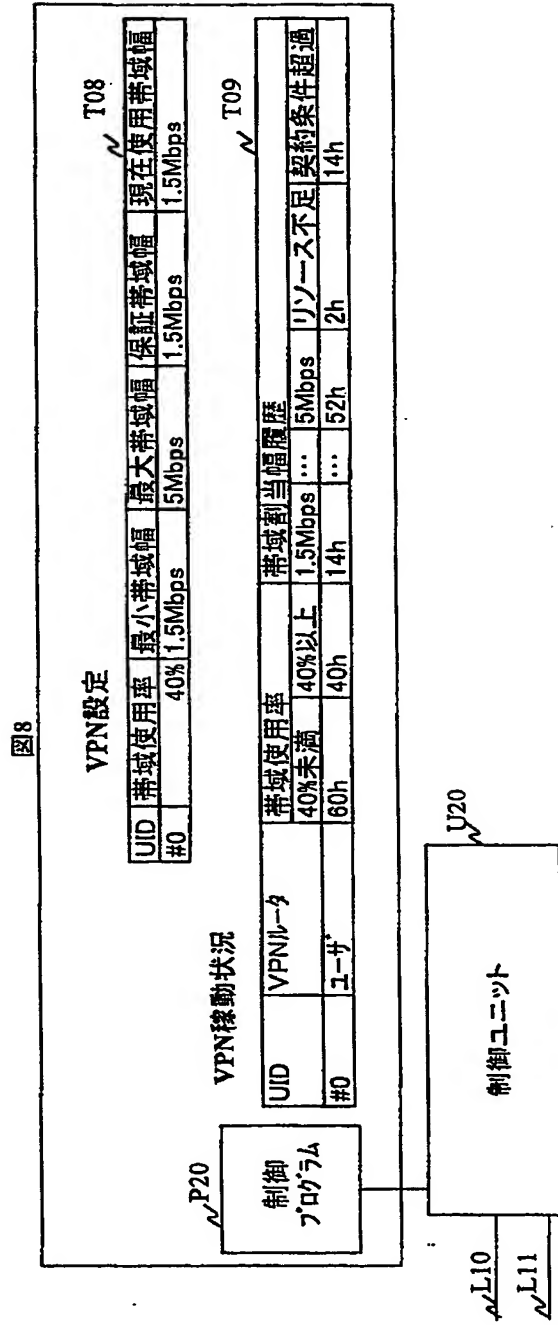
図6



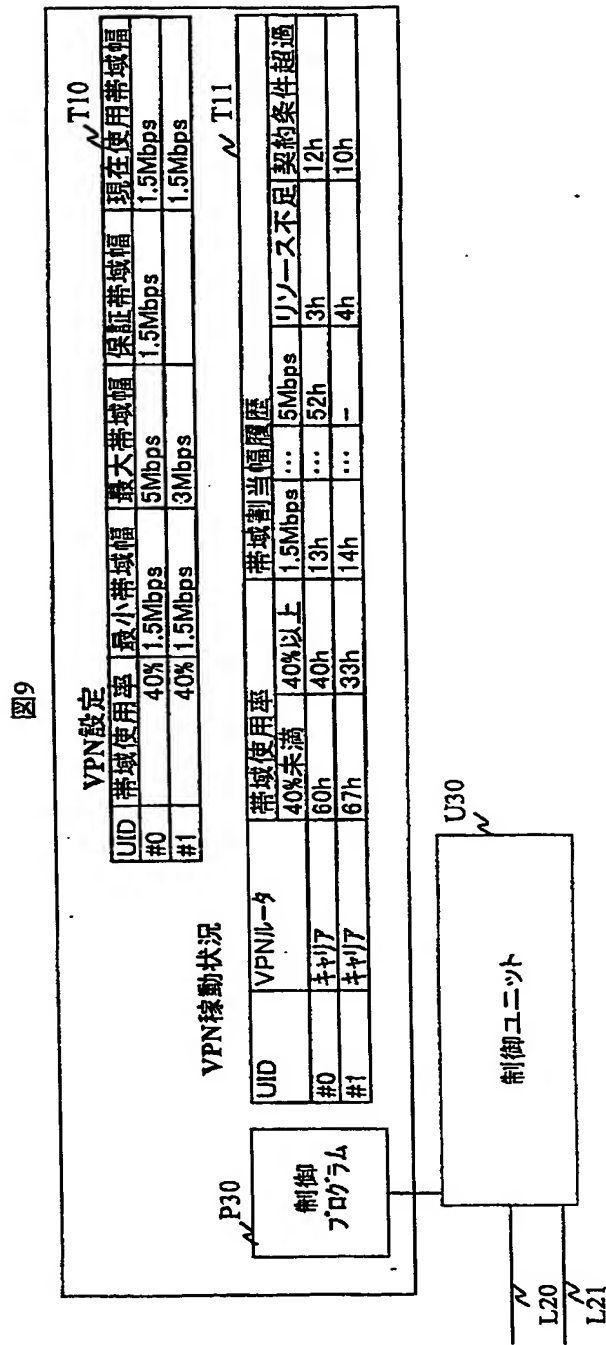
【図 7】



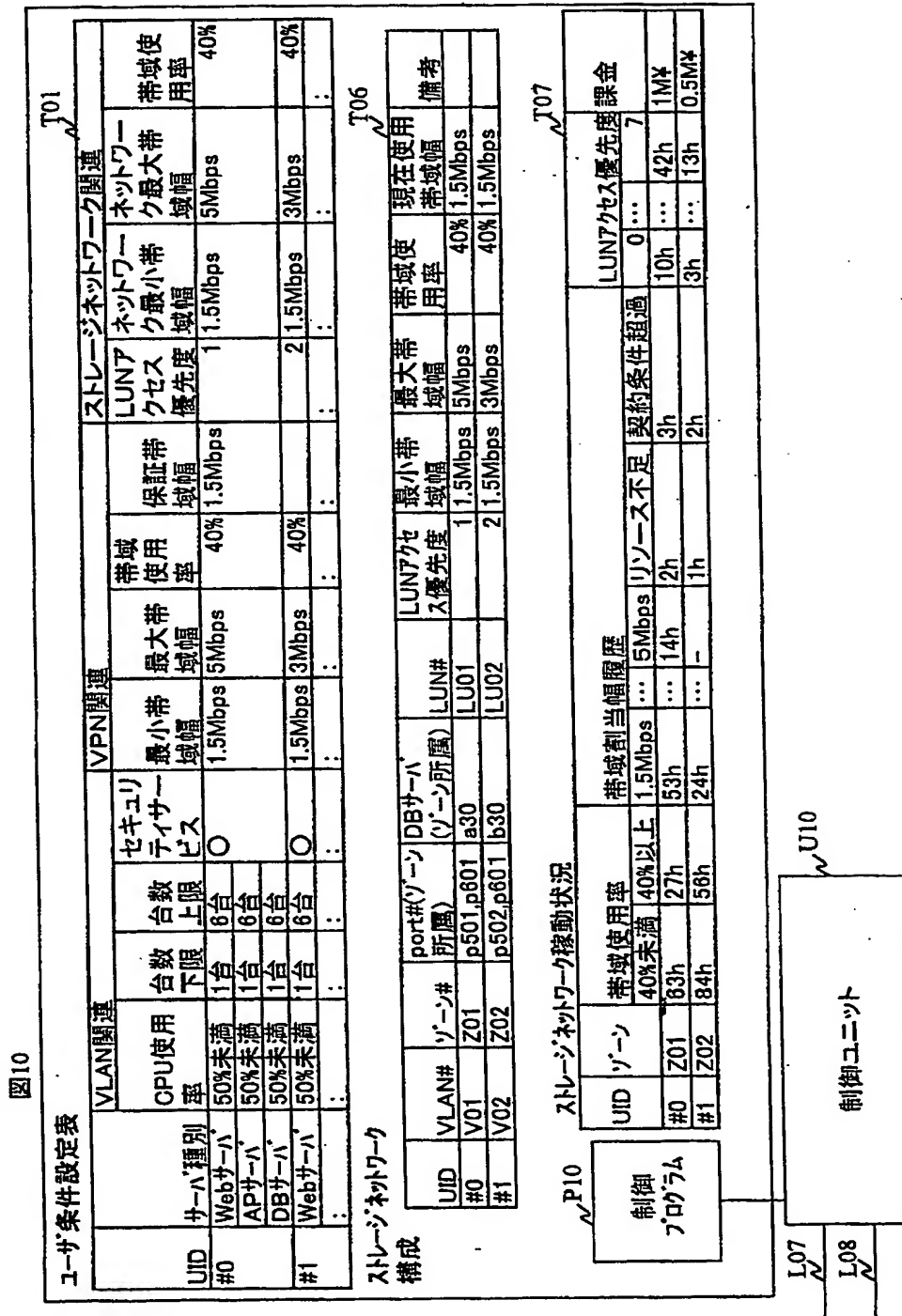
【図 8】



【図9】

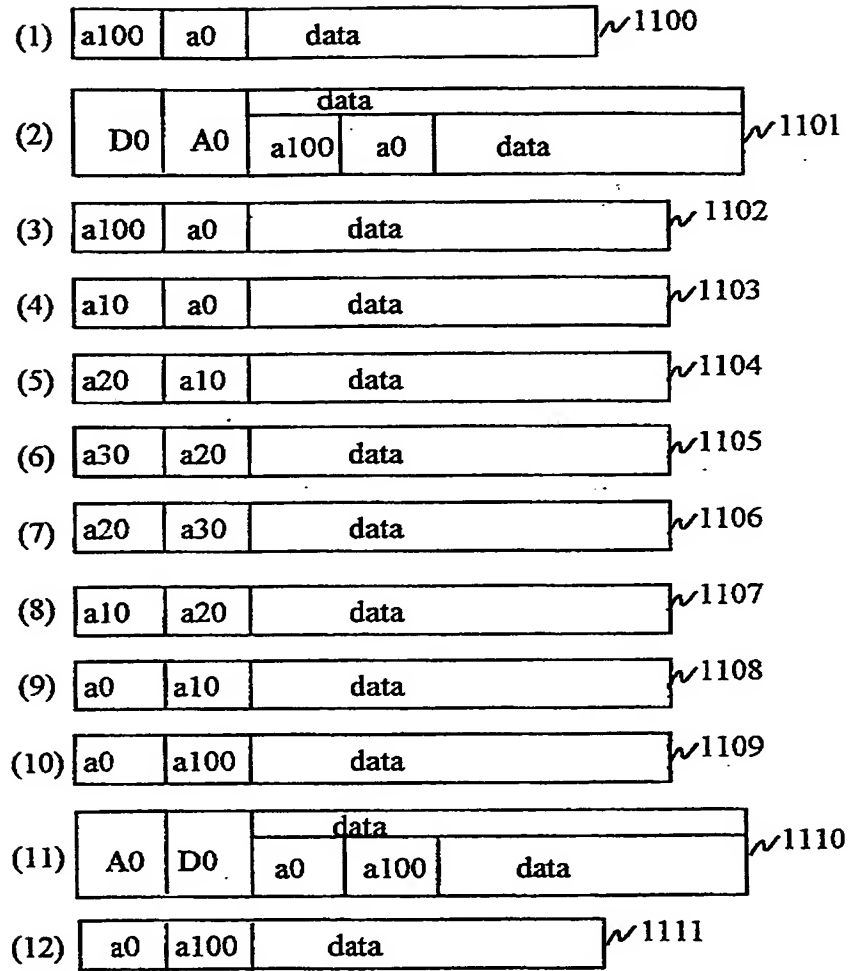


【図 1 0】



【図 1 1】

図11



【図 1 2】

図12 U01

サービスレベル条件入力画面(オプション選択)

セキュリティオプション

専用のVLAN及びVPNを設定 不要 希望

☐ ☒

信頼性オプション

ネットワーク通信帯域保証を設定 不要 希望

☐ ☒

【図 1 3】

図13 U02

サービスレベル条件入力画面

代表アドレス

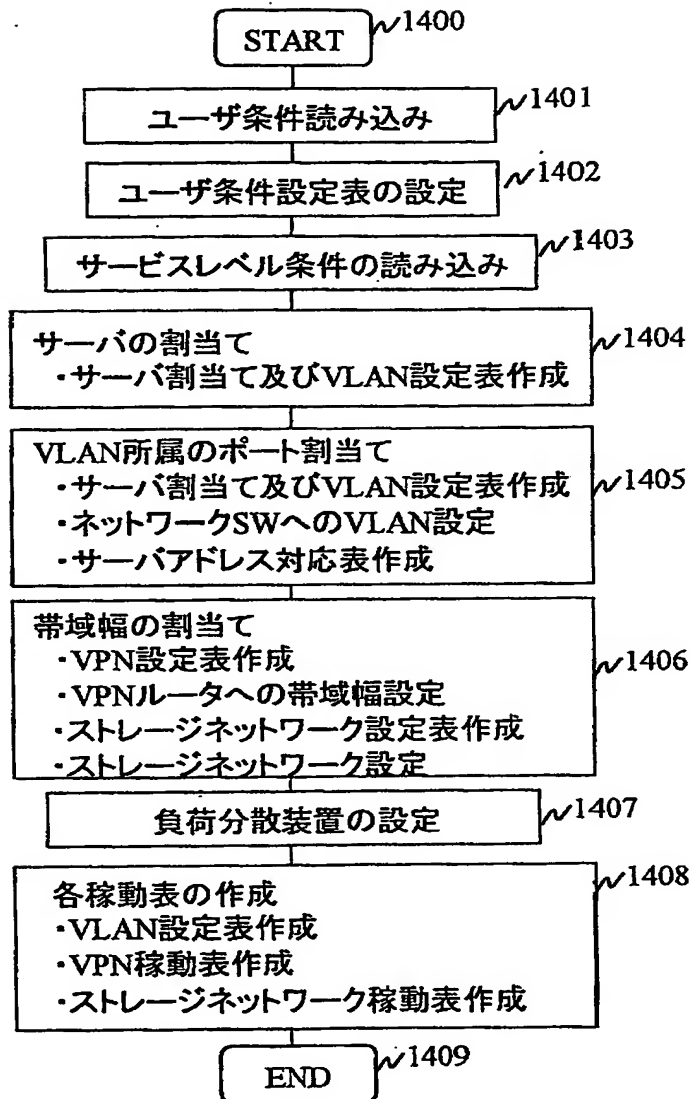
使用サーバ種別	サーバ数		使用条件	
	下限	上限	CPU稼働率	..
webサーバ <input checked="" type="checkbox"/>	<input type="text" value="1"/> 台	<input type="text" value="6"/> 台	<input type="text" value="50%未満"/>	<input type="text"/>
APサーバ <input checked="" type="checkbox"/>	<input type="text" value="1"/> 台	<input type="text" value="6"/> 台	<input type="text" value="50%未満"/>	<input type="text"/>
DBサーバ <input checked="" type="checkbox"/>	<input type="text" value="1"/> 台	<input type="text" value="6"/> 台	<input type="text" value="50%未満"/>	<input type="text"/>

U03 ☒ VPNオプション (選択の場合記入)

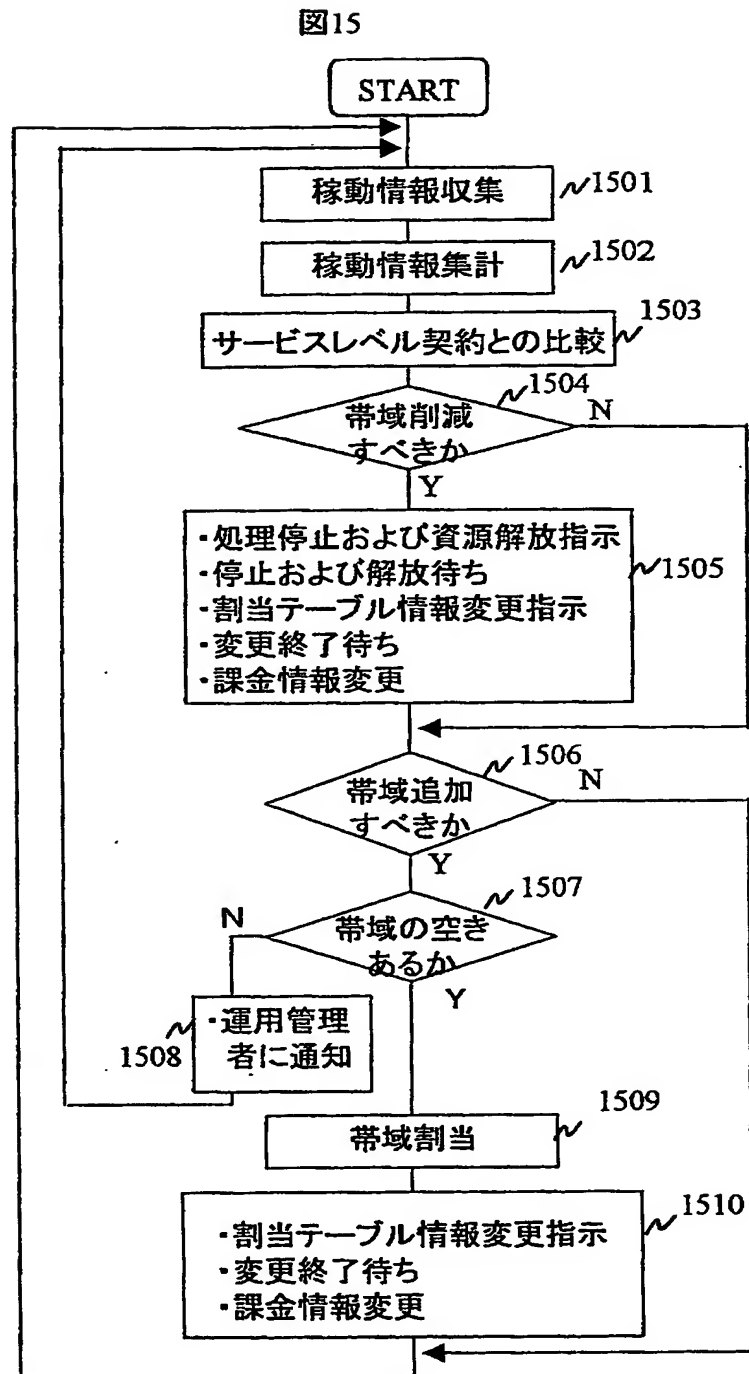
ネットワーク帯域幅		使用条件
最小	最大	帯域使用率
<input type="text" value="1.5"/> Mbps	<input type="text" value="5"/> Mbps	<input type="text" value="40%未満"/>
ストレージネットワーク帯域幅		使用条件
最小	最大	帯域使用率
<input type="text" value="1.5"/> Mbps	<input type="text" value="5"/> Mbps	<input type="text" value="40%未満"/>

【図 1 4】

図14

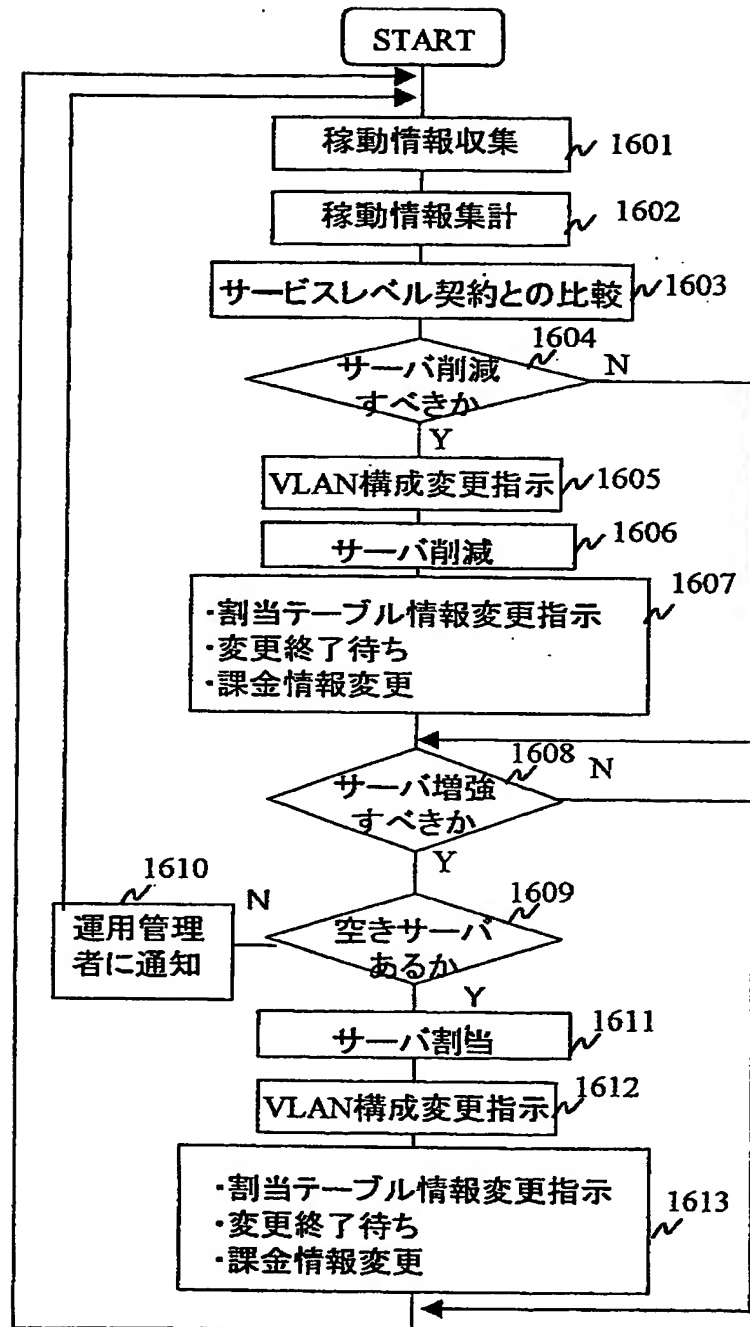


【図15】

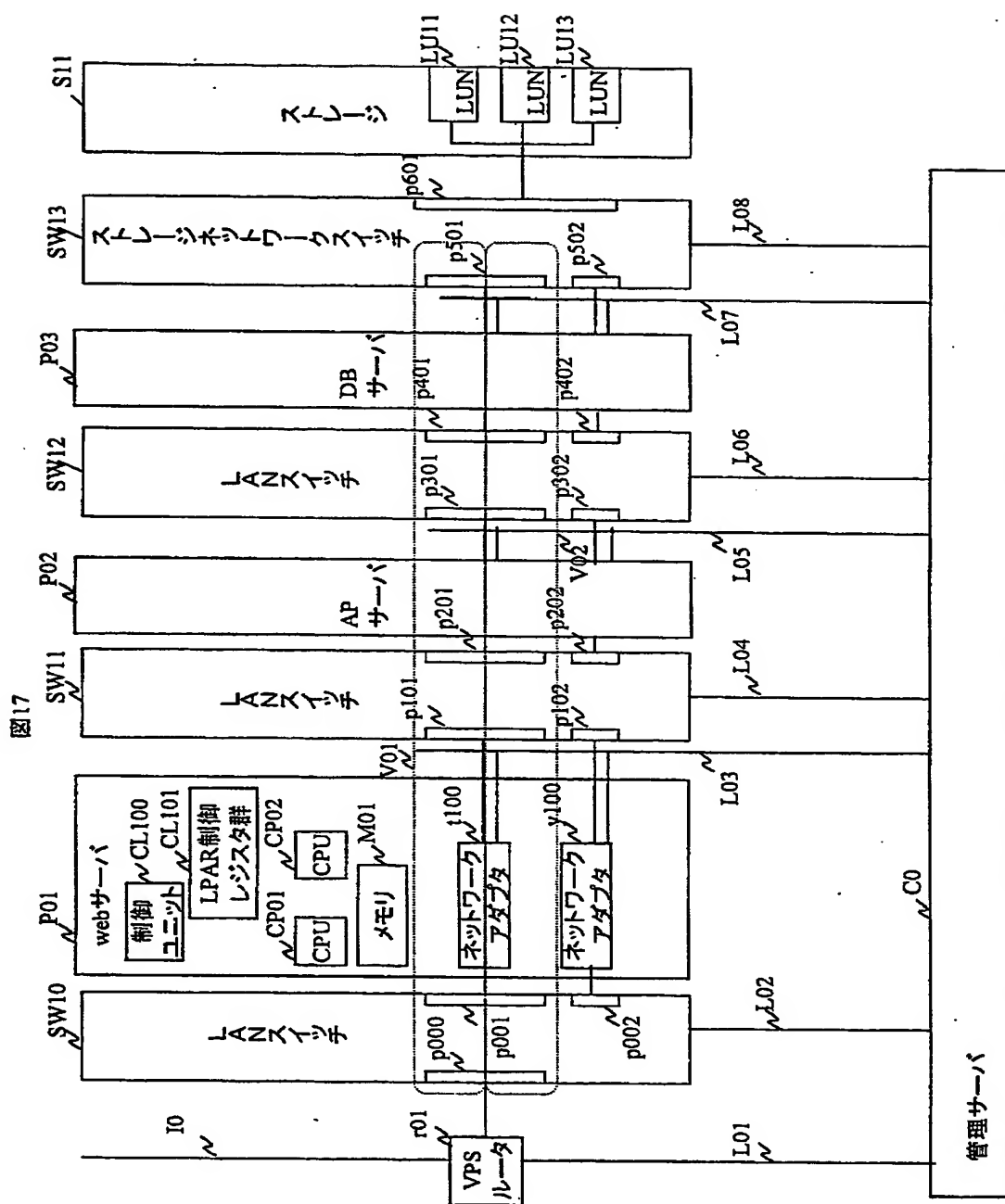


【図 1 6】

図16



【図 17】



【図 18】

図18 U05

サービスレベル条件入力画面(オプション画面)

セキュリティオプション

・専用のVLAN及びVPNを設定 不要 希望

☐ ☒

信頼性オプション

・ネットワーク通信帯域保証を設定 不要 希望

☐ ☒

【図 19】

図19 U06

サービスレベル条件入力画面

アドレス Web AP DB

使用サーバ種別	CPU割当率		使用条件	
	下限	上限	CPU稼働率	..
webサーバ <input checked="" type="checkbox"/>	<input type="text" value="20"/> %	<input type="text" value="70"/> %	<input type="text" value="50%未満"/>	<input type="text"/>
APサーバ <input checked="" type="checkbox"/>	<input type="text" value="20"/> %	<input type="text" value="70"/> %	<input type="text" value="50%未満"/>	<input type="text"/>
DBサーバ <input checked="" type="checkbox"/>	<input type="text" value="20"/> %	<input type="text" value="70"/> %	<input type="text" value="50%未満"/>	<input type="text"/>

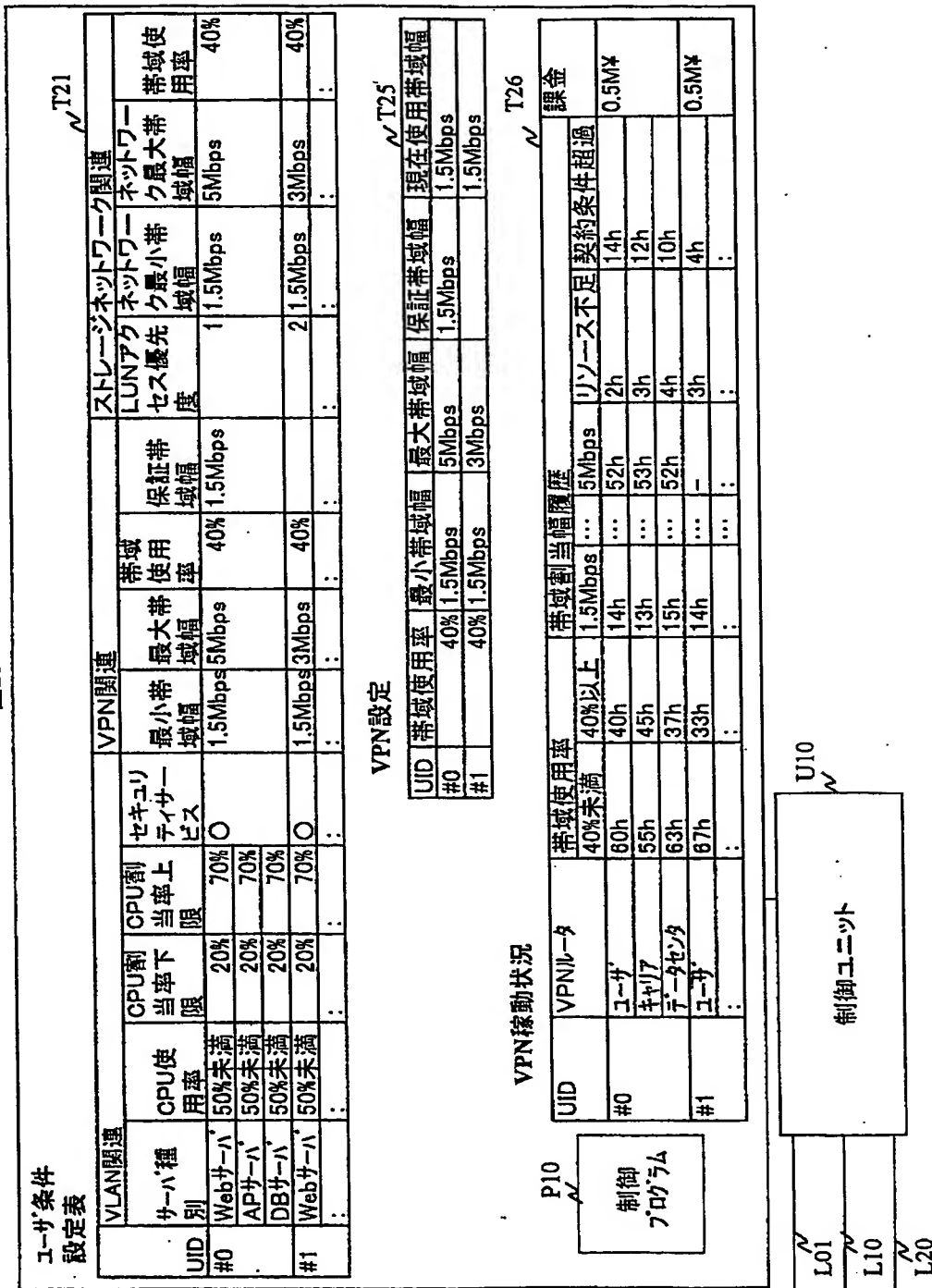
☒ VPNオプション (選択の場合記入)

ネットワーク帯域幅		使用条件
最小	最大	帯域使用率
<input type="text" value="1.5"/> Mbps	<input type="text" value="5"/> Mbps	<input type="text" value="40%未満"/>
ストレージネットワーク帯域幅		使用条件
最小	最大	帯域使用率
<input type="text" value="1.5"/> Mbps	<input type="text" value="5"/> Mbps	<input type="text" value="40%未満"/>

U07

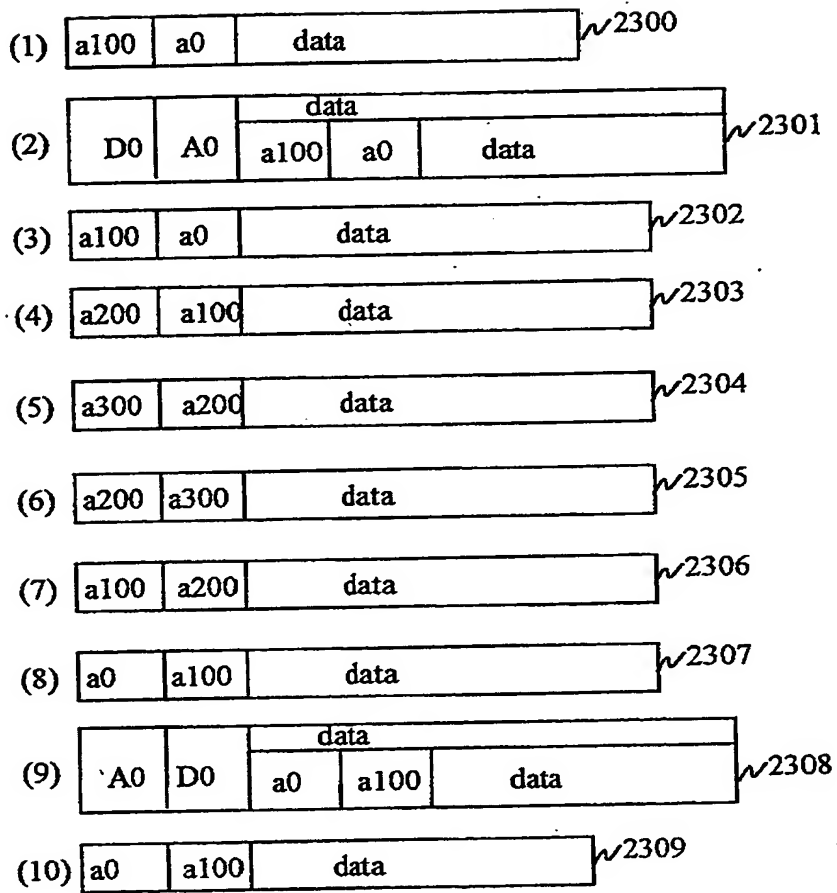
【図 2 1】

図21

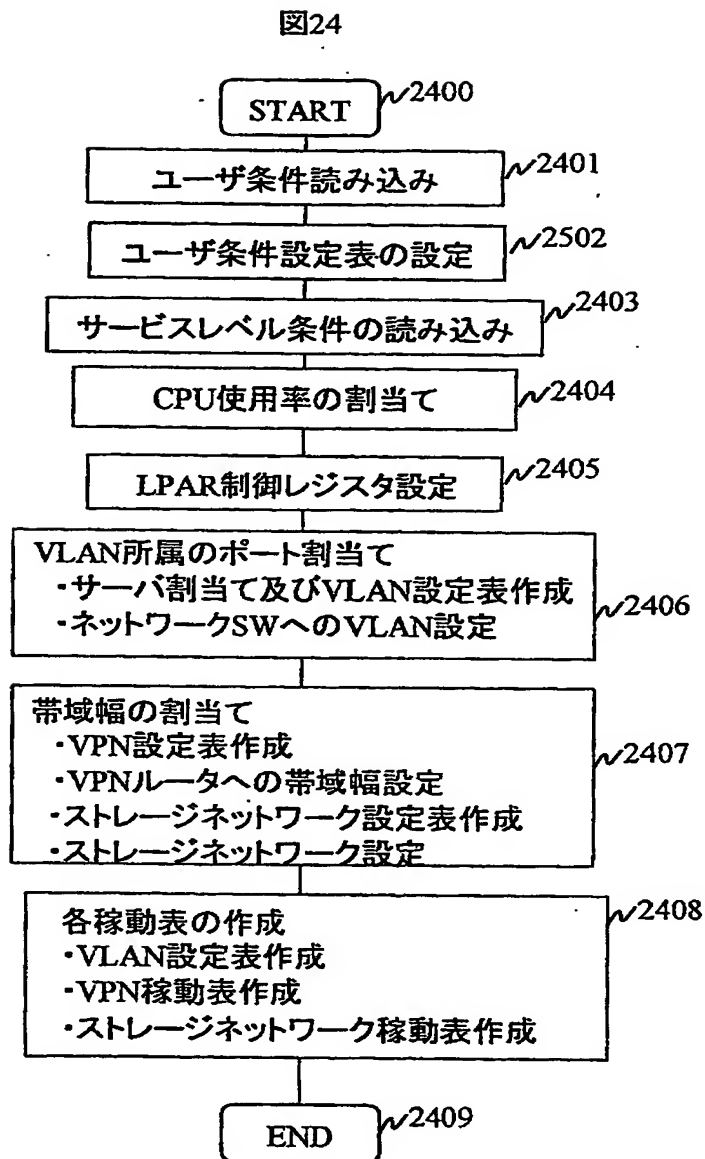


【図 2 3】

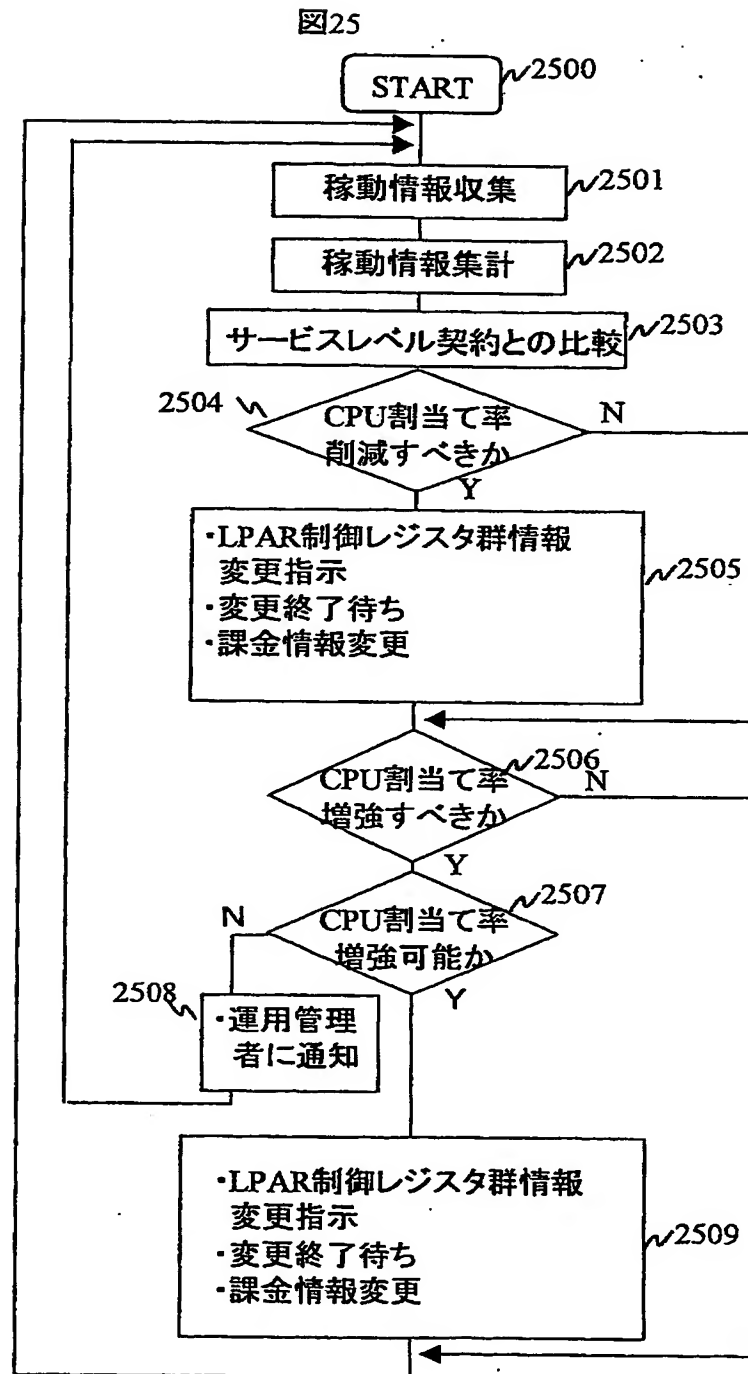
図23



【図 2 4】

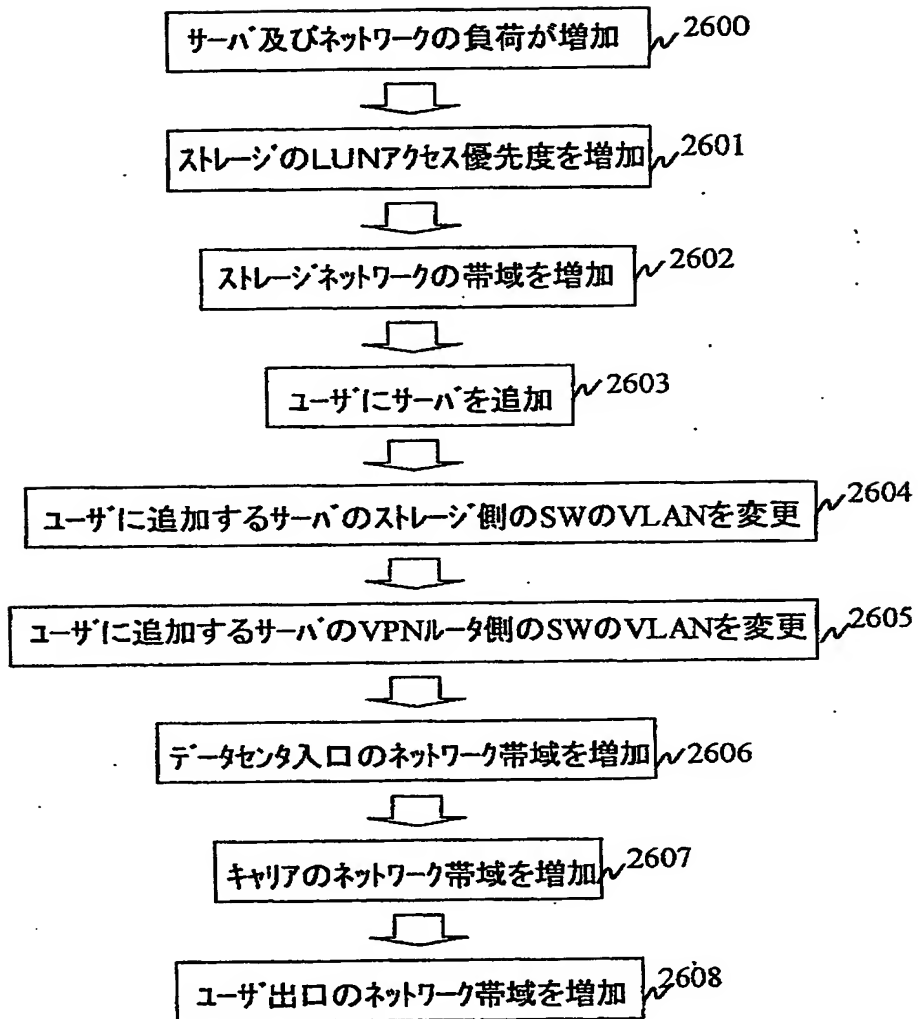


【図 25】



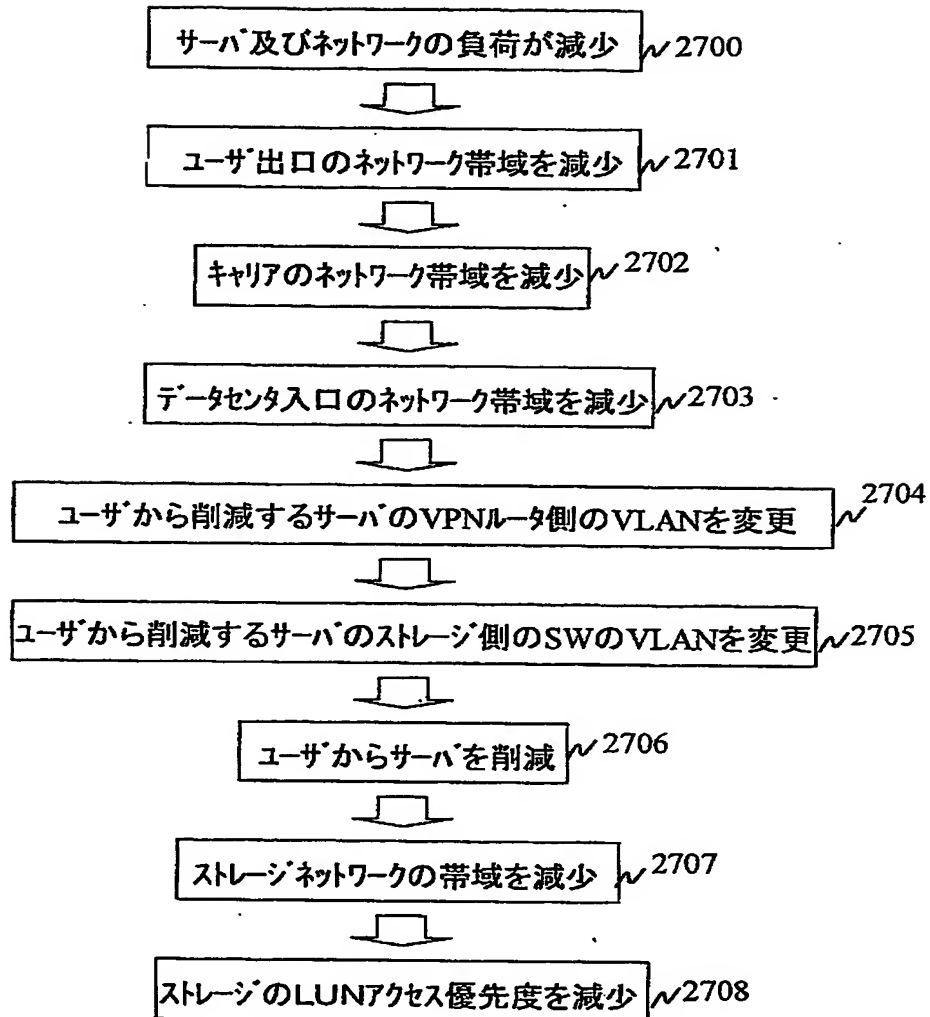
【図 26】

図26

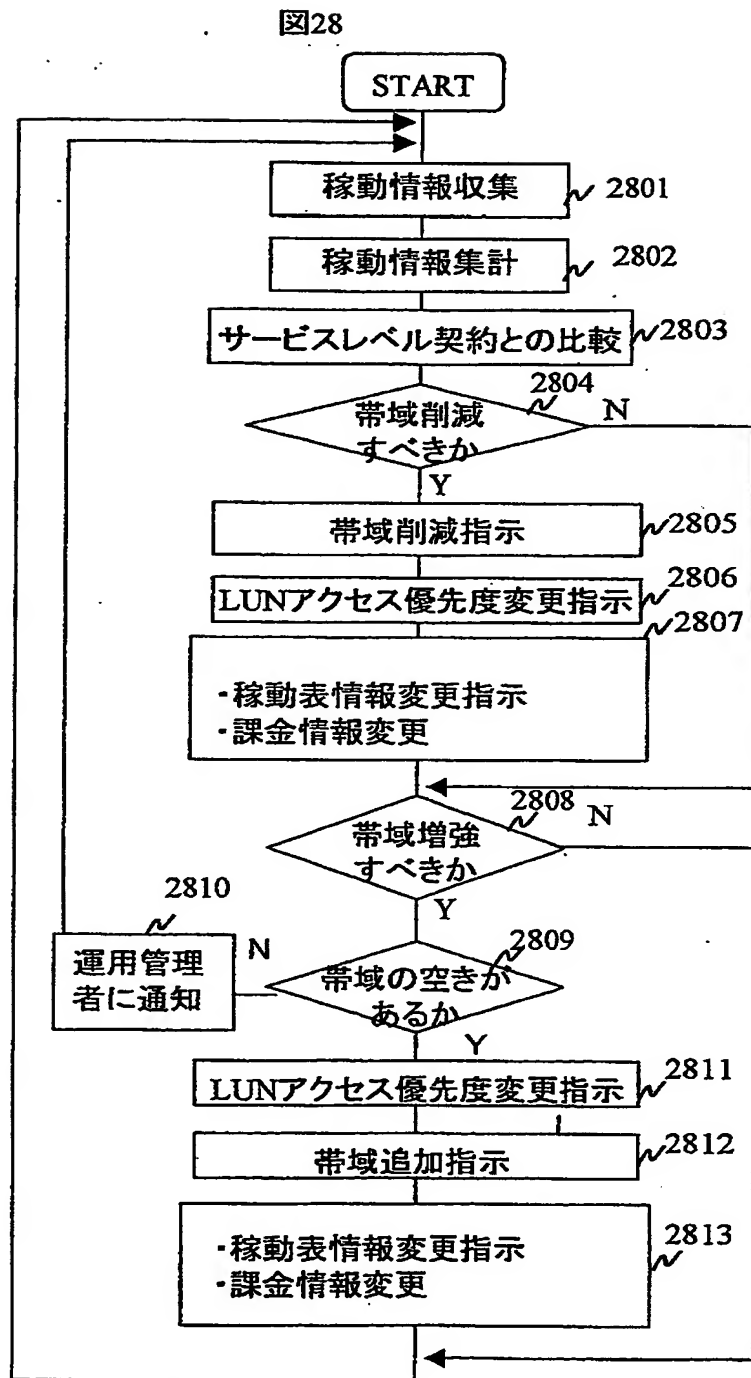


【図 27】

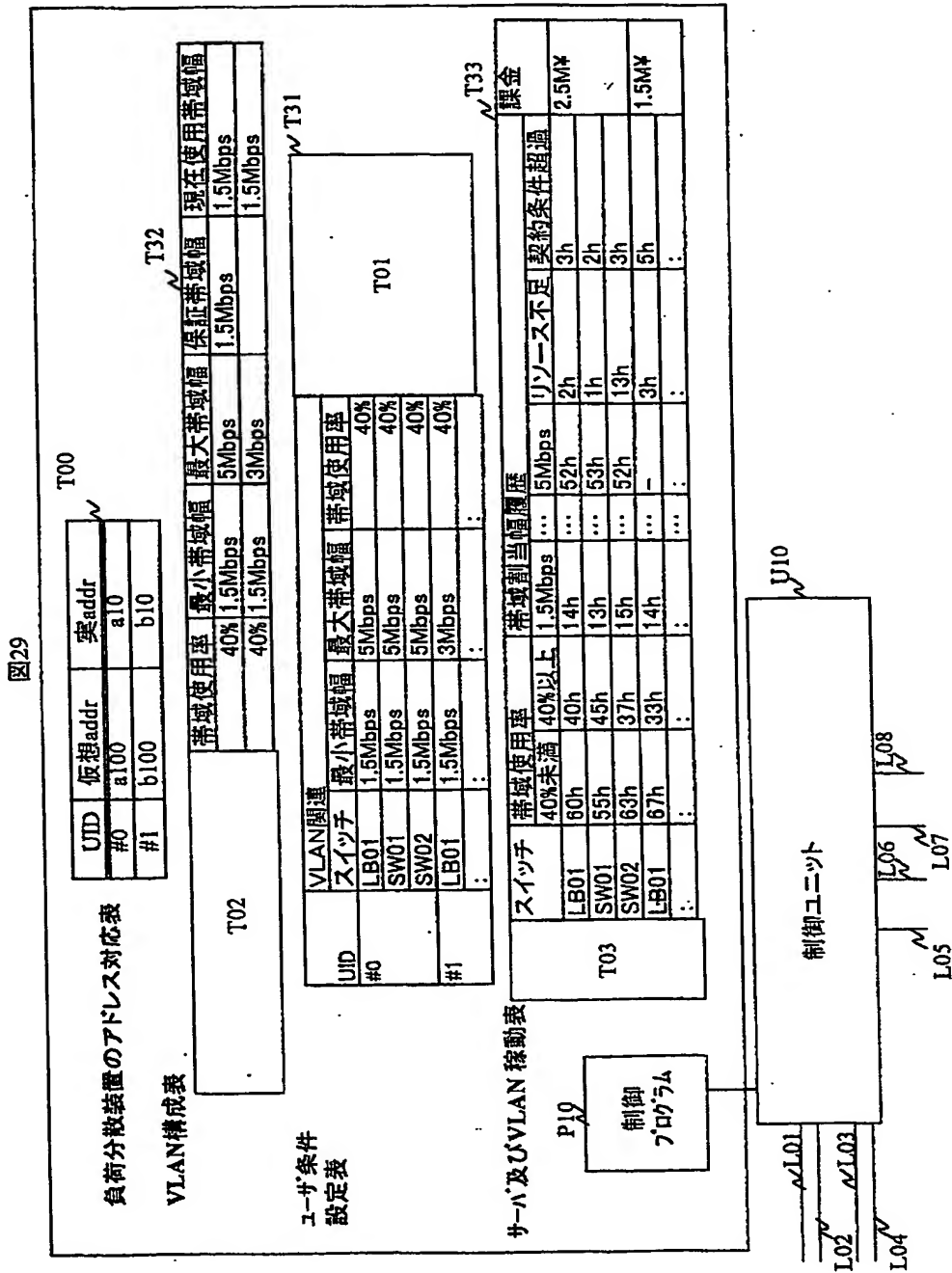
図27



【図 2 8】

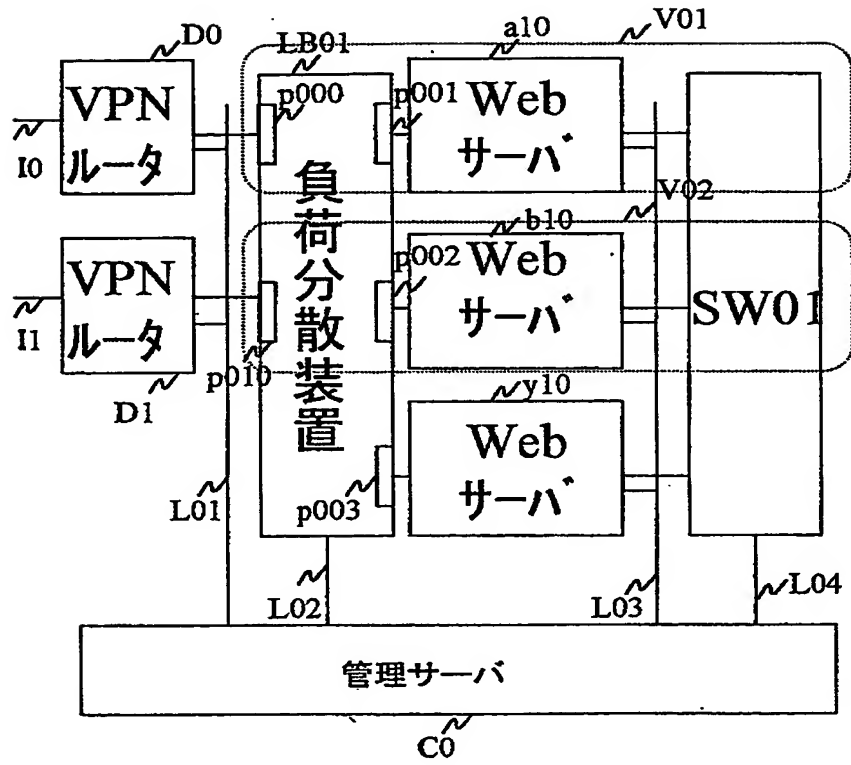


【図 29】



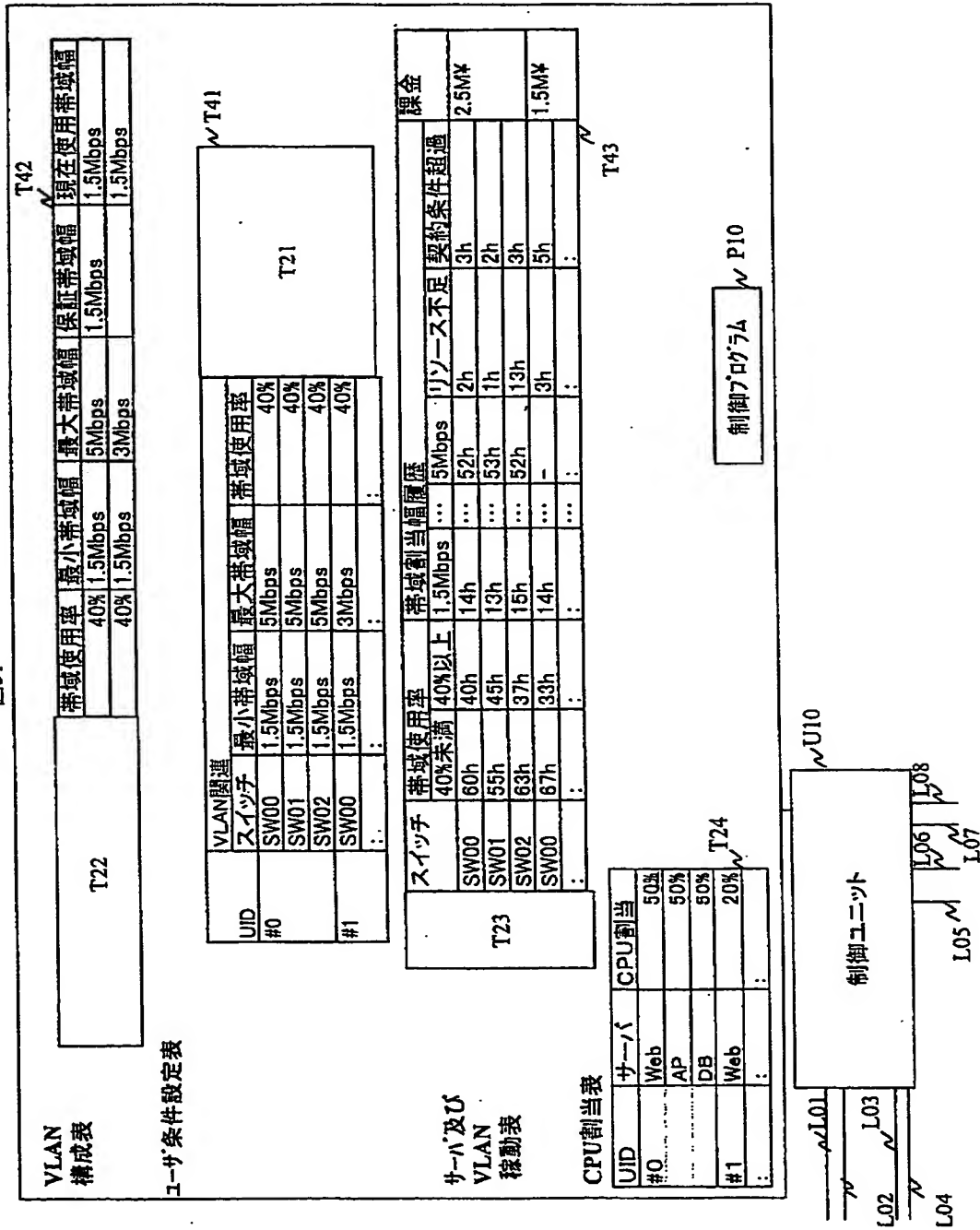
【図 3 0】

図30

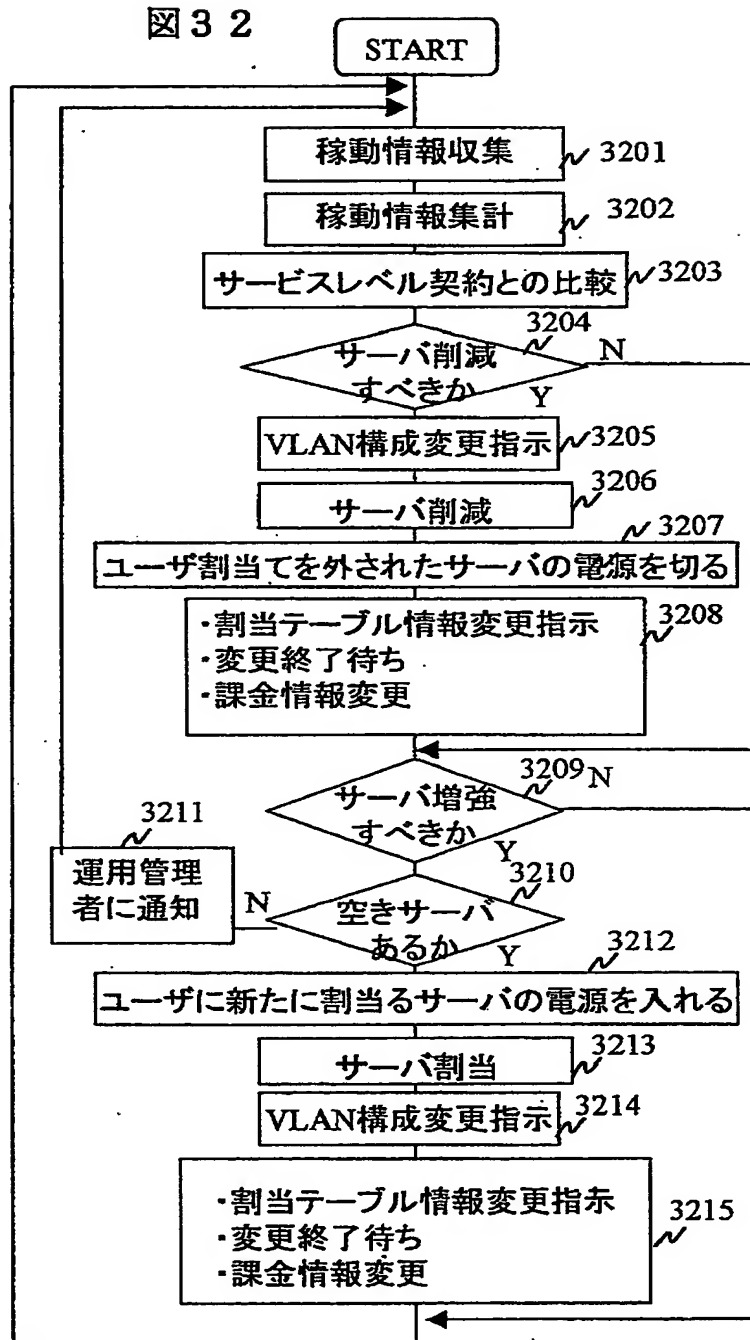


【図 31】

図31



【図32】



【書類名】 要約書

【要約】

【課題】 データセンタにおいて、ユーザの負荷が変動した時に、負荷に応じてユーザに対する資源の割当てを動的に変更し、また、各ユーザ毎のセキュリティを保つ。

【解決手段】 データセンタの管理サーバC0上の制御プログラムP10は、ユーザ企業毎に複数のネットワークスイッチを含む専用のVLANを割当てるようにVLAN構成表(T02)を作成し、ユーザに割当てられている負荷分散装置LB01やネットワークスイッチSW01、SW02の当該ポートをユーザ専用のVLANに設定する。また、ユーザからデータセンタまではVPNを設定し、VLANタギングの技術を使うことによって、ユーザからデータセンタまでの間ではユーザのセキュリティは確保される。さらに、P10はユーザごとのサービスレベル契約に沿って作られたユーザ条件設定表(T01)と、計算機の稼動状況モニタ結果(VLAN稼動表T03中のCPU使用率履歴)を比較し、契約条件未達時は計算機の割当及びVLAN構成を動的に変える。具体的にはT02、03を変更し、負荷分散装置LB01及びネットワークスイッチSW01、SW02におけるVLANの設定変更を行う(Web層の場合)。さらにP10は、それに基づく課金情報に関するパラメータ(T03中サーバ割当て履歴)を変更する。

【選択図】 図2

特2001-312115

認定・付加情報

特許出願の番号	特願2001-312115
受付番号	50101493590
書類名	特許願
担当官	第七担当上席 0096
作成日	平成13年10月11日

<認定情報・付加情報>

【提出日】 平成13年10月10日

次頁無

出 願 人 履 歴 情 報

識別番号 [000005108]

1. 変更年月日 1990年 8月31日
[変更理由] 新規登録
住 所 東京都千代田区神田駿河台4丁目6番地
氏 名 株式会社日立製作所